



Helsinki University of Technology  
Department of Engineering Physics and Mathematics  
Laboratory of Physics

---

## Master's Thesis

# Quantum Cryptography Protocol Based on Sending Entangled Qubit Pairs

Olli Ahonen

Supervisor: Prof. Risto Nieminen  
Instructor: Dr. Mikko Möttönen

<b>Author:</b>	Olli Ahonen
<b>Department:</b>	Engineering Physics and Mathematics
<b>Major:</b>	Materials Physics
<b>Minor:</b>	Software Systems
<b>Title:</b>	Quantum Cryptography Protocol Based on Sending Entangled Qubit Pairs
<b>Otsikko:</b>	Kietoutuneisiin qubitpareihin perustuva kvantti-salausmenetelmä
<b>Chair:</b>	Tfy-44 (Materials Physics)
<b>Supervisor:</b>	Professor Risto Nieminen
<b>Instructor:</b>	Dr. Tech. Mikko Möttönen

The quantum key distribution protocol BB84, published by C. H. Bennett and G. Brassard in 1984, describes how two spatially separated parties can generate a random bit string fully known only to them by transmission of single-qubit quantum states. Any attempt to eavesdrop on the protocol introduces disturbance which can be detected by the legitimate parties.

In this Master's Thesis a novel modification to the BB84 protocol is analyzed. Instead of sending single particles one-by-one as in BB84, they are grouped and a non-local transformation is applied to each group before transmission. Each particle is sent to the intended receiver, always delaying the transmission until the receiver has acknowledged the previous particle on an authenticated classical channel, restricting eavesdropping to accessing the quantum transmission one particle at a time. Hence, an eavesdropper cannot undo the non-local transformation perfectly. Even if perfect cloning of quantum states was possible the state of the group could not be cloned.

We calculate the maximal information on the established key provided by an intercept-resend attack and the induced disturbance for different transformations. We observe that it is possible to significantly reduce the eavesdropper's maximal information on the key—to one eighth of that in BB84 for a fixed, reasonable amount of disturbance. We also show that the individual access to the particles poses a fundamental restriction to the eavesdropper, and discuss a novel attack type against the proposed protocol.

<b>Keywords:</b>	Quantum cryptography, Quantum key distribution, BB84, Entanglement
------------------	--

<b>Pages:</b>	75	<b>Date:</b> March 1 <sup>st</sup> , 2007
---------------	----	---

<b>Approved:</b>	<b>Location:</b>
------------------	------------------

<b>Tekijä:</b>	Olli Ahonen	
<b>Osasto:</b>	Teknillisen fysiikan ja matematiikan osasto	
<b>Pääaine:</b>	Materiaalifysiikka	
<b>Sivuaine:</b>	Ohjelmistojärjestelmät	
<b>Otsikko:</b>	Kietoutuneisiin qubitipareihin perustuva kvantti-salausmenetelmä	
<b>Title:</b>	Quantum Cryptography Protocol Based on Sending Entangled Qubit Pairs	
<b>Professuuri:</b>	Tfy-44 (Materiaalifysiikka)	
<b>Valvoja:</b>	Professori Risto Nieminen	
<b>Ohjaaja:</b>	TkT Mikko Möttönen	
<p>C. H. Bennett ja G. Brassard julkaisivat vuonna 1984 BB84:ksi kutsutun menetelmän, jolla toisistaan etäällä olevat osapuolet voivat luoda satunnaisen bittijonon, jonka vain he tuntevat kokonaan. Menetelmä hyödyntää yksiqubittilojen ominaisuuksia. Kaikki mahdolliset salakuunteluyritykset aiheuttavat häiriötä, jonka perusteella salakuuntelu voidaan havaita.</p> <p>Tässä diplomityössä tutkitaan uudenlaista BB84:ään perustuvaa menetelmää. Sen sijaan, että yksittäisiä hiukkasia lähetettäisiin erikseen kuten BB84:ssä, ne ryhmitellään, ja kunkin ryhmän hiukkasten tilat kiedotaan erityisellä muunnoksella. Kietoutuneet hiukkaset lähetetään toiselle osapuolelle siten, että kunkin hiukkasen lähetystä lykätään kunnes edellisestä lähetyksestä on saatu kuittaus. Tämä rajoittaa salakuuntelun yhteen hiukkaseen kerrallaan, joten salakuunteliija ei pysty perumaan tehtyä muunnosta täydellisesti. Vaikka täydellinen kvantttilojen kopioiminen olisi mahdollista, kiedotun ryhmän tilaa ei voida kopioida.</p> <p>Laskemme eri muunnoksille sieppaus-uudelleenlähetys -hyökkäyksellä saatavan maksimaalisen tiedon avaimesta ja kvanttikanavassa aiheutetun häiriön. Havaitsemme, että maksimaalista tietoa on mahdollista rajoittaa huomattavasti, jopa kahdeksasosaan BB84:n vastaavasta arvosta. Näytämme, että salakuuntelun rajoittaminen yhteen hiukkaseen kerrallaan luo perustavanlaatuisen esteen salakuuntelulle. Esitämme myös uudenlaisen hyökkäyksen ehdotettua menetelmää vastaan.</p>		
<b>Avainsanat:</b>	Kvanttikryptografia, Avaimenjako, BB84, Kietoutuminen	
<b>Sivuja:</b>	75	<b>Päiväys:</b> 1. maaliskuuta 2007
<b>Hyväksytty:</b>	<b>Sijainti:</b>	

# Acknowledgements

I would like to kindly thank my instructor Dr. Tech. Mikko Möttönen for all his constructive advice and readily available guidance on this Thesis. I am grateful to all the members of the Quantum many-body physics group for creating a positive and pleasant working atmosphere, and to Prof. Risto Nieminen and Docent Ari Harju for the marvellous opportunity to work in the group. I would also like to thank the members of the positron group of our laboratory for their invaluable help in the beginning of my academic career.

Special thanks belong to my parents, without whose continual support I cannot imagine having achieved so much in my life, and to my big sister and my little brother for all the joyous moments they have provided during the years. Finally, I wish to thank my fiancée Helena for her unconditional support and the happiness she brings to my life.

*“Work like you’d live forever.  
Love like you’d die tomorrow.”  
–Seneca*

*Otaniemi, March 1st 2007*

Olli Ahonen

# Contents

<b>Acknowledgements</b>	<b>iii</b>
<b>Table of Contents</b>	<b>iv</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Classical and Quantum Information</b>	<b>7</b>
2.1 Elementary probability theory . . . . .	8
2.2 Shannon entropy and mutual information . . . . .	9
2.3 Error correction of shared data . . . . .	10
2.3.1 A simple error-correcting protocol . . . . .	11
2.3.2 The Cascade error-correcting protocol . . . . .	11
2.4 The unit of quantum information . . . . .	12
2.4.1 Realization of a qubit . . . . .	12
2.4.2 Superposition . . . . .	14
2.5 Entanglement . . . . .	14
2.5.1 Entanglement of formation and concurrence . . . . .	15
2.6 Quantum measurement . . . . .	16
2.6.1 Projective measurements . . . . .	16
2.6.2 Positive operator-valued measures . . . . .	17
2.7 Quantum cloning . . . . .	18

2.7.1	The no-cloning theorem . . . . .	18
2.7.2	Optimal cloning . . . . .	19
<b>3</b>	<b>Quantum Key Distribution</b>	<b>22</b>
3.1	BB84 protocol . . . . .	23
3.1.1	Transmission . . . . .	24
3.1.2	Measurement . . . . .	25
3.1.3	Basis reconciliation . . . . .	26
3.1.4	Issues introduced by non-ideal equipment . . . . .	27
3.1.5	Attacks . . . . .	29
3.1.6	Privacy amplification . . . . .	42
3.2	Other protocols . . . . .	42
3.2.1	Einstein-Podolsky-Rosen protocol . . . . .	42
3.2.2	Two-state protocol . . . . .	43
3.2.3	Six-state protocol . . . . .	44
3.2.4	Adjusted basis probabilities protocol . . . . .	44
<b>4</b>	<b>Analysis and Results</b>	<b>45</b>
4.1	Proposed modification to the BB84 protocol . . . . .	45
4.2	Product-state approximation of an entangled qubit pair . . . . .	47
4.2.1	Theory . . . . .	48
4.2.2	Solution . . . . .	49
4.2.3	Results . . . . .	50
4.3	Analysis of an intercept-resend attack . . . . .	51
4.3.1	Parametrization of $U$ . . . . .	51
4.3.2	Explicit matrices . . . . .	53
4.3.3	Simulation . . . . .	54
4.3.4	Results . . . . .	61
4.4	EPR-pair attack . . . . .	67

<b>5</b>	<b>Conclusions</b>	<b>70</b>
----------	--------------------	-----------

	<b>Bibliography</b>	<b>72</b>
--	---------------------	-----------

# Chapter 1

## Introduction

In human societies, the desire of two parties to communicate in secret dates back at least as far as the first known societies themselves [1]. When the two parties are not in perfect isolation, that is, when the messages they exchange may become available to outsiders, the best known technique to achieve secrecy is *cryptography*. Cryptography is about concealing the meaning of communicated messages from any unintended recipients. This is traditionally achieved by the following scheme: The legitimate parties share a relatively small amount of secret information, a *key*, based upon which the sender chooses a transformation, and the receiver another transformation that perfectly undoes the effect of the former. Each message is transformed, i.e. *encrypted*, by the sender before sending the message, and then re-transformed, i.e. *decrypted*, by the receiver to recover the original message. Only receivers in possession of the correct key know exactly which decrypting transformation to apply.

Today, secrecy of communication is not compromised by lack of secure encryption-decryption schemes, but is rather hindered by the complicated problem of delivering the needed encryption-decryption keys safely. This fact is nicely exemplified by a cryptographic protocol known as the one-time pad, first proposed by J. Mauborgne [2]. The one-time pad scheme requires that the two communicating parties share in advance a secret key that is as long as the message they wish to transmit. Assuming that the key and the message are in binary form, i.e., strings of zeroes and ones, both the sender and the receiver apply the bitwise exclusive-or (XOR) operation: Each bit in the message to be sent is flipped if and only if the corresponding bit in the key



has value one. After reception, the receiver performs exactly the same operation, and recovers the original message. As long as the key is never reused, the one-time pad is unbreakable. That is, without knowledge of the key, the communication is perfectly secret.

The one-time pad keys are far from a relatively small amount of secret information, and hence agreeing on them is in general a daunting task. Therefore, the one-time pad as such is not of much practical value, despite its extreme security. Instead of insisting on perfect security, contemporary protocols use a rather short key many times but involve transformations more complicated than a single bitwise XOR. These protocols are, in principle, vulnerable to careful analysis of a large amount of captured, although encrypted, communication. With key lengths of 128 to 256 bits, however, cryptographic protocols employing, e.g., the Advanced encryption standard (AES) algorithm, are considered secure enough [3].

One way of solving the problem of key distribution is to utilize asymmetric *public-key encryption* which is in widespread use today. In public-key encryption schemes, two parties desiring secret communication need not share any secret information in advance. The intended receiver of the messages can give the sender a *public key* which the sender uses to encrypt messages. Messages encrypted with the public key can only be decrypted with a corresponding *private key*. Public-key encryption is usually used to exchange keys for symmetric encryption-decryption schemes that use only one key, for example, AES-based protocols.

In public-key encryption schemes, deducing the private key from the public key is generally considered *hard*, i.e., the deduction would take an overwhelming amount of time on any computer. However, this conjecture has never been proved. Thus, it is possible that this deduction can be performed in a reasonable amount of time. Moreover, it is known that the public-key to private-key deduction is feasible on a large-scale *quantum computer*, but the demanding task of constructing such a device remains yet to be accomplished. Because of the possibility of recording encrypted transmissions, the security of not only future but also all past public-key-encrypted communication is based on a conjecture of the difficulty of the key deduction.

The history of *quantum cryptography* can be considered to begin in 1969. By then, the peculiar properties of quantum physics, discovered in the early decades

of the 20th century, had not only been developed into a rigorous theory, but also increasingly adopted by scientists. In 1969, Stephen Wiesner introduced<sup>1</sup> the idea of forgery-proof quantum banknotes [5]. These banknotes would contain a serial number encoded by the issuing bank into quantum states of individual particles. By the laws of quantum mechanics, anyone unaware of the details of the encoding could not produce copies of the banknotes. Although this idea of uncloneable sequence of numbers is not an essential primitive or function in quantum cryptography, the next milestone in the field owes much to its insight [6].

This milestone is the *quantum key distribution protocol* of C. H. Bennett and G. Brassard published in 1984 [7]. The protocol, referred to as BB84, describes how two spatially separated parties can generate a random bit string, a sequence of zeroes and ones, fully known only to them. The protocol exploits properties of single quanta predicted by quantum physics. The sender transmits a sequence of individual particles, e.g., photons, each in one of four equally probable quantum states. Any eavesdropping on the states of the particles between the sender and the intended receiver inevitably introduces disturbance to the transmission, which can later be detected by the legitimate parties. In addition, an eavesdropper has only bounded information on the established bit sequence. These properties are guaranteed by the laws of physics: An eavesdropper can only gain knowledge on the transmission by measurements. The states of the particles are chosen so that any physically conceivable measurement will never provide the eavesdropper with full knowledge on the transmission, and will almost certainly disrupt the transmission. The protocol requires that the sender and the receiver can communicate via an authenticated<sup>2</sup> classical channel, e.g., a phone line. The classical channel can be assumed public, e.g., wire-tapping is allowed on a phone line.

Since it was first introduced, several variations of and modifications to the BB84 protocol have been proposed. These include, for example, modifying the number of states allowed to the transmitted particles [8, 9], adjusting the probabilities of the individual states of the particles [10], transmitting the individual states on more than one particle [11], and exploiting quantum-mechanical spatial superposition [12].

---

<sup>1</sup>Wiesner's proposition was not, however, published until 1983 [4].

<sup>2</sup>On an authenticated channel an outsider cannot pose as a legitimate user.

---

The so-called Einstein-Podolsky-Rosen (EPR) protocols offer a different, yet in many ways equivalent, approach to quantum key distribution [13]. In EPR protocols, the individual particles are not transmitted from sender to receiver but emanate from a separate source. This source always emits two particles in an *entangled* state, one particle for each party of the protocol. Entangled particles exhibit correlations independent of their spatial distance. These correlations are exploited by the participants of the protocol to establish a secret random bit sequence. Once again, it is possible to detect if anyone has tampered with the source or the particles before their reception. An authenticated classical channel is needed in this protocol, as well.

As such, none of the quantum-cryptographic protocols mentioned above provide the participants with an error-free perfectly secret bit sequence—one that no-one else has any knowledge of. They rather allow the two parties to share a bit sequence, and guarantee that no-one else has information on the sequence above some fixed value. Furthermore, their sequences do not match perfectly because of unavoidable noise and possible eavesdropping on the transmitted quantum states. A decent amount of errors can be corrected safely by communication over a public classical channel. Moreover, the participants may perform *privacy amplification*: they exchange further information over the classical channel while shortening their bit sequence, and thus reduce any eavesdropper’s knowledge of the sequence to an arbitrarily low value. Hence, the legitimate parties can finally obtain a shared, perfectly secret, error-free bit sequence.

Above, we discussed how quantum cryptography can be used to send secret random bit strings between two parties. What is the value of this capability in terms of secret communication? Indeed, if they are strictly random, these secret shared bit sequences provided by the quantum protocols described above can—after error correction and privacy amplification—be directly used as keys in classical symmetric cryptography already in everyday use. This essential and non-trivial key-distribution function is what quantum cryptography in its modern form is most suited for. Hence, quantum cryptography and quantum key distribution are often used synonymously. The practical applications of these protocols can safely replace risky public-key-encrypted key distribution methods.

Quantum cryptography became reality in 1992, as C. H. Bennett *et al.* experimentally implemented the BB84 protocol for the first time [14]. The protocol was completed between parties 30 cm apart—a distance not of much interest in a commercial application. Since the first experimental realization, quantum key distribution has been successfully carried out over distances of tens of kilometers [15, 16]. However, quantum cryptography is still plagued by the difficulty of realizing the protocol over longer distances. Practical applications invariably use photons as the carrier of the quantum states. Photons may be transported either in optical fibre or in free space, i.e., earth’s atmosphere. For either choice, the rapid decay of faint light pulses prohibits secure quantum cryptography over distances above 100 km. [17, 18]

In this Master’s Thesis, a novel modification to the BB84 protocol is analyzed. This modification is outlined as follows: Instead of sending the single particles one-by-one, they are grouped and a transformation coupling the particles is applied to each group before transmission. This transformation is assumed to be known by the sender and receiver, as well as any eavesdropper. After the transformation, the particles are sent to the intended receiver, but always delaying the transmission until the receiver has acknowledged receiving the previous particle on the authenticated classical channel. This restricts eavesdropping to accessing the quantum transmission one particle at a time. But because a transformation involving a group of particles was applied, the eavesdropper generally cannot undo that transformation perfectly. Moreover, even if the eavesdropper was capable of cloning the states of the individual particles for herself<sup>3</sup>, she could not clone the state of the entire group formed by the sender. The legitimate receiver, on the other hand, can undo the transformation used by the sender because he or she has simultaneous access to all the particles of a group. Not all quantum transformations involving a group of particles are such that they cannot be reversed one particle at a time; the transformation has to be *non-local*. The aim of this Thesis is to find out exactly which non-local transformation allows the legitimate users of the modified protocol to gain the maximal advantage over an eavesdropper. Furthermore, we restrict ourselves to the case where the group size is two particles, i.e., the particles are handled in pairs.

Chapter 2 reviews the concepts and results of classical and quantum information

---

<sup>3</sup>In fact, we show in Sec. 2.7 that this is not possible.

theory needed in subsequent chapters. Chapter 3 defines and describes in detail the aspects of quantum key distribution relevant to our studies. The analysis of the modified protocol is presented in Ch. 4 which includes the obtained results. Finally, Ch. 5 concludes this Thesis with a summary and suggestions for future research.

## Chapter 2

# Classical and Quantum Information

This chapter presents mathematical tools of classical and quantum information needed in our studies. The reader is assumed to be familiar with elementary quantum mechanics which will not be discussed here. In the first section, we briefly review some useful results of probability theory. In Sec. 2.2, we define information-theoretic *entropy* and its derivative, *mutual information*. Entropy is indisputably the central concept in classical information theory. Mutual information enables us to give quantitative expression to statements such as: “An adversary has knowledge on a secret key.” Section 2.3 discusses correcting errors in transmitted data due to an imperfect channel between two parties. Error correction is accomplished by exchanging further information about the erroneous data.

The latter part of this chapter discusses topics specific to quantum information. Sections 2.4 and 2.5 introduce the quantum analog of the bit, namely the *qubit*, and the properties that most notably distinguish qubits and classical bits. A short discussion concerning the physical realizations of a qubit is also included. Section 2.6 reviews means to read existing qubits, i.e., quantum-mechanical measurements. Finally, copying, or cloning, of quantum information is discussed in Sec. 2.7.

## 2.1 Elementary probability theory

The theory of probability can be formulated on the basis of the notion of a *random variable*. A random variable  $X$  may assume a number of values, and the value  $X$  has assumed is denoted by  $x$ . The probability with which  $X$  assumes the value  $x$ , is denoted by  $p(X = x)$ , which may also be written  $p(x)$ . If the possible values  $X$  may take are  $x_1, x_2, \dots, x_n$ , the *probability distribution* of  $X$  is  $p_X := (p(x_1), p(x_2), \dots, p(x_n)) := (p_1, p_2, \dots, p_n)$ . Random variables relevant to this Thesis always take their value from a finite set. The probability that two distinct random variables  $X$  and  $Y$  assume values  $x$  and  $y$ , respectively, is denoted by  $p(X = x \text{ AND } Y = y)$  or, in short,  $p(x, y)$ . The probability that  $X$  assumes  $x$  or  $Y$  assumes  $y$ , or both, is denoted by  $p(X = x \text{ OR } Y = y)$ . The notation also generalizes to more than two random variables.

For any two random variables  $X$  and  $Y$ , and their respective outcomes  $x$  and  $y$ , we have

$$p(X = x \text{ OR } Y = y) = p(x) + p(y) - p(x, y) . \quad (2.1)$$

*Conditional probability* is defined by

$$p(x|y) := \frac{p(x, y)}{p(y)} , \quad (2.2)$$

and gives the probability that  $X$  assumes value  $x$ , when it is known that  $Y$  has taken value  $y$ . When  $p(y) = 0$ , we define  $p(x|y) = 0$ . When  $Y$  has no effect on the outcome of  $X$ ,  $p(x|y) = p(x)$ , and vice versa. Hence, two random variables are *independent* if and only if  $p(x, y) = p(x)p(y)$ . Equation (2.2) implies *Bayes' theorem* which states that

$$p(x|y) = p(y|x) \frac{p(x)}{p(y)} . \quad (2.3)$$

This expression is often amended by writing  $p(y)$  in the form given by another direct consequence of Eq. (2.2), the *law of total probability*:

$$p(y) = \sum_x p(y|x)p(x) . \quad (2.4)$$

From these equations, the following rules can be derived for random variables  $A$ ,  $B$ ,

and  $C$  and their respective outcomes  $a$ ,  $b$ , and  $c$ :

$$p(a|b) = \sum_c p(a, c|b) , \quad (2.5)$$

$$p(a, b|c) = p(a|b, c)p(b|c) , \quad (2.6)$$

$$p(a|b, c) = p(b|a, c) \frac{p(a|c)}{p(b|c)} . \quad (2.7)$$

## 2.2 Shannon entropy and mutual information

Entropy is described with respect to an *information source*, or equivalently, a random variable. Entropy quantifies the average information gain per use of an information source, or per instance where we let a random variable  $X$  assume a value in accordance with its probability distribution  $p_X$ . Entropy describes our uncertainty of the random variable *before* it has assumed its value, or alternatively, how many *units of information* we have acquired *after* we have learned its value. These two views are equivalent.

The choice for the unit of information is embedded in the definition of entropy. In this Thesis, the unit of classical information is always a bit. Hence, logarithms are always taken to base two:  $\log(\cdot) := \log_2(\cdot)$ , unless otherwise stated.

The Shannon entropy of a random variable  $X$  with probability distribution  $(p_1, p_2, \dots, p_n)$  is defined by

$$H(X) := H(p_1, p_2, \dots, p_n) = - \sum_{j=1}^n p_j \log p_j . \quad (2.8)$$

An impossible event should not contribute to entropy, and we therefore define  $0 \log(0) := 0$ . Note that entropy achieves its minimum, zero, if one of the probabilities  $p_j = 1$ . For a given number of possible outcomes  $n$ , entropy is maximized if the probability distribution is flat, i.e.,  $p_j = \frac{1}{n}$  for all  $j \in \{1, 2, \dots, n\}$ . The maximal value is  $\log n$ . The entropy of the simplest random variable that is still meaningful, one having only two possible outcomes with probabilities  $p$  and  $1 - p$ , is known as *binary entropy*. Its explicit formula is

$$H_{\text{bin}}(p) := -p \log p - (1 - p) \log(1 - p) . \quad (2.9)$$



To quantify the average combined information gain of the outcomes  $x$  and  $y$  of two random variables  $X$  and  $Y$ , we define the *joint entropy* by

$$H(X, Y) := - \sum_{x, y} p(x, y) \log p(x, y) . \quad (2.10)$$

The above equation implies that  $H(Y, X) = H(X, Y)$ .

The mutual information of two random variables  $X$  and  $Y$  describes how much information they have in common, and is defined by

$$I(X, Y) := H(X : Y) := H(X) + H(Y) - H(X, Y) . \quad (2.11)$$

It is clear that  $I(Y, X) = I(X, Y)$ . It also holds that  $I(X, Y) = 0$  if and only if  $X$  and  $Y$  are independent. Equation (2.11) can be intuitively justified as follows: The first two terms,  $H(X)$  and  $H(Y)$ , represent the information content of  $X$  and  $Y$ . Any information common to them is included in both terms, while their individual information content is included only in the respective term. It follows that common or joint information is counted twice and non-common information once. Therefore, the third term,  $-H(X, Y)$ , subtracts the individual and common information of the variables, leaving only their mutual information.

## 2.3 Error correction of shared data

Consider the following scenario: Two parties, Alice and Bob, share data as a result of some completed protocol. For simplicity, we assume the data is a string of bits. The string contains errors, e.g., Alice has 011010 where Bob has 010010, there is an error in the third bit. Alice and Bob wish to correct all errors by exchanging further data, disclosing as little information as possible about the string to any other parties. The theoretical minimum of bits that Alice and Bob have to exchange is

$$r = n(-p \log p - (1 - p) \log(1 - p)) = nH_{\text{bin}}(p) , \quad (2.12)$$

where  $n$  is the length of the string and  $p$  is the individual probability of error for each slot in the string [17]. The result is based on Shannon's noiseless coding theorem, for which unfortunately only a non-constructive proof is known [19]. That is, we know an error-correcting protocol requiring the exchange of only  $r$  bits is possible, but we do not know the details of any such protocol.

### 2.3.1 A simple error-correcting protocol

As an example of error correction, we describe a very simple and inefficient error-correcting protocol. In this context, inefficiency means that parts of the original data must be discarded, and that the protocol exchanges much more than  $r$  bits for a realistic value of  $p$ . The protocol works as follows: Alice randomly chooses pairs of slots in the string, and sends Bob the slot numbers and her XOR value of the bits in the two slots. Bob replies with his XOR value of the corresponding bits. If Alice and Bob's XOR values match, they keep the bit in the first slot and discard the second-slot bit. If their XOR value does not match, they discard both bits. The longer Alice and Bob iterate this procedure, the smaller the probability of an error in their string becomes. [18]

### 2.3.2 The Cascade error-correcting protocol

As a second example of error-correction schemes, we review a protocol significantly more advanced than that described above. The so-called Cascade protocol, presented by G. Brassard and L. Salvail, is practical and efficient, preserves the length of the original data, and nearly achieves the bound in Eq. (2.12) [20]. Let  $A = (A_1, A_2, \dots, A_n)$  be Alice's and  $B = (B_1, B_2, \dots, B_n)$  Bob's bit string, where  $A_j, B_j \in \{0, 1\}$ .

In the first *pass* of the protocol, Alice and Bob choose an integer  $k_1$ , and group their strings into blocks of length  $k_1$ . Both Alice and Bob compute the parity of each block, i.e., sum up the  $k_1$  bits of each block modulo 2. Alice then sends the parities of her blocks to Bob. When Bob discovers that the parity of one of his blocks,  $B_l$ , differs from Alice's corresponding parity, Bob knows that there is an odd number of bit errors in block  $B_l$ . Now Alice and Bob initiate the Binary protocol, in which they interactively and recursively find the erroneous bit in the block. The Binary protocol works as follows: Alice sends Bob the parity of the first half of the block. Bob compares this to the parity of the first half of his block. If these parities agree, the error must be in the second half, and if they disagree, the error is in the first half. Binary is then applied to the block half containing the error. The recursion ends and one erroneous bit is corrected, when the block size reaches a small enough

value. At this point, the first pass is complete, leaving all of Bob's blocks with either zero or an even number of bit errors.

In each pass  $j > 1$  Alice and Bob agree on a random shuffling of the bits, and apply the steps of the first pass to the string, with block size  $k_j$ . Each time an error is corrected, there must be previously treated blocks, whose amount of bit errors just changed from even to odd. Let  $\mathcal{K}$  denote the set of these blocks. Alice and Bob apply the Binary protocol to the smallest block in  $\mathcal{K}$ , and repeat this until all blocks in  $\mathcal{K}$  are treated. This ends pass  $j$ . The block sizes  $k_i$  and the number of executed passes must be optimized so that the probability of any remaining errors is small enough and at the same time the leakage of information to outsiders is minimal. The parameters depend on the bit error rate  $p$ .

## 2.4 The unit of quantum information

Classical information is most conveniently stored and manipulated as bits, and, in classical computer science, the bit is the most commonly used unit of information [21]. The bit has a quantum analog, the qubit<sup>1</sup>, which in turn is the most widely used unit of quantum information. In principle, any quantum system that has at least two states can be considered a qubit: Given any multilevel system, two of its states are simply labeled  $|0\rangle$  and  $|1\rangle$ , in the Dirac bracket notation. This two-state subsystem constitutes the qubit. Furthermore, one can make the distinction between *logical* and *physical qubits*. A logical qubit is a mathematical concept, an aid in the theoretical discussion of quantum information processing, whereas physical qubits actually span the suitable physical subspaces for logical qubits. In this Thesis, the word qubit refers to a logical qubit.

### 2.4.1 Realization of a qubit

D. DiVincenzo has compiled a list of criteria for a particular physical system in order for it to be useful as a qubit in a functioning quantum computer [22]. This often-quoted list is known as the DiVincenzo criteria, and it applies in many respects to

---

<sup>1</sup>To distinguish a classical bit from a qubit, it is sometimes labeled 'cbit'.

quantum cryptography, as well. The first criterion states that the system should be scalable and the qubits should be well characterized. That is, the relevant physical parameters of the qubit should be known, e.g., the internal Hamiltonian, states of the physical qubit, and couplings external fields. Secondly, it should be possible to initialize a relevant array of qubits to a known, low-entropy state, e.g.,  $|00\dots\rangle$ . The third criterion concerns aspects of the protocol presented in this Thesis. It states that decoherence of qubit states should progress much slower than the unitary operations, that is, quantum gates<sup>2</sup>, applied to the qubits. Obviously, computation is not possible if the information contained in the qubits irreversibly leaks into the environment between elementary operations. The fourth criterion is related to the theory of quantum computation. It states that for the proposed realization of the qubit there should exist a set of quantum gates that is universal, i.e., a set with which any unitary operation is achievable. Finally, the result of a quantum information processing task should be attainable: The fifth criterion of DiVincenzo requires the individual qubits to be measurable with high fidelity.

In addition to the list presented above, DiVincenzo points out two requirements for successful quantum communication. A realization of the qubit, when used in communication, must be such that it is possible to convert stationary qubits, used for local computation or data storage, into flying qubits that are the ones exchanged by two communicating parties. The conversion from flying to stationary qubits should also be achievable. There is, of course, no restriction on the flying and stationary qubits being the same physical system. In addition, it should be possible to transmit flying qubits between specified locations with a low error rate.

For instance, the polarization of a photon can be treated as a flying qubit. The vertical polarization, relative to a fixed frame of reference, may be chosen to be the state  $|0\rangle$ , and the horizontal polarization to be the state  $|1\rangle$ . For further example, Elliott *et al.* [23] present a network, in which secure quantum key distribution is achieved with photons carrying the flying qubits. The authors report an error rate of 6-8% for the qubits.

---

<sup>2</sup>Unitary operations targeted to qubits are called gates in quantum computation. They are the quantum analogy of logical gates targeted to cbits.

### 2.4.2 Superposition

What really distinguishes quantum bits from classical bits, is the possibility of *superposition*: The qubit may occupy state  $|0\rangle$ , state  $|1\rangle$ , or a linear combination of these two, which is always of the form

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.13)$$

where the complex numbers  $\alpha$  and  $\beta$  satisfy  $|\alpha|^2 + |\beta|^2 = 1$  to ensure that the state is normalized. For  $\alpha, \beta \neq 0$ , the state of the qubit is said to be a superposition of  $|0\rangle$  and  $|1\rangle$ .

## 2.5 Entanglement

Not only single qubits can occupy a superposition state, but any number of qubits can jointly occupy a superposition state. If this many-qubit superposition state is inexpressible as a tensor product of individual qubit states, the qubits are said to occupy an *entangled* state. Entanglement has no classical analogy, since collections of classical bits in any state are always expressible by specifying the state of its components individually, whereas this is not true for collections of quantum bits. For example, the two-qubit normalized state<sup>3</sup>  $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$  is not an entangled state, because it can be decomposed as  $|\Psi\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle + |1\rangle)$ . In contrast, the state  $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  is entangled, as it cannot be written in a tensor-product form.

Entanglement can be considered as an elementary resource in quantum information processing [24, 25], and hence one should be able to express the amount of entanglement in a given quantum state. However, there is no general agreement on how to quantify entanglement. As an example of entanglement measures we briefly review the *entanglement of formation* for a qubit pair, summarizing the work of W. K. Wootters [26]. An extensive list of entanglement measures is given, for example, in Ref. [25].

---

<sup>3</sup>Notation:  $|\Psi_1\rangle \otimes |\Psi_2\rangle := |\Psi_1\rangle|\Psi_2\rangle := |\Psi_1\Psi_2\rangle$ , where  $\otimes$  is the Kronecker product.

### 2.5.1 Entanglement of formation and concurrence

Suppose a bi-partite quantum system consisting of subsystems  $A$  and  $B$  is in state  $\rho$ . State  $\rho$  has a number of pure-state decompositions  $\{p_i, |\psi_i\rangle\}$ , for which

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \quad (2.14)$$

For each pure state  $|\psi_i\rangle\langle\psi_i|$  of the system, the entanglement of formation is

$$E(\psi_i) := -\text{Tr}(\rho_A \log \rho_A) = -\text{Tr}(\rho_B \log \rho_B), \quad (2.15)$$

where  $\rho_A = \text{Tr}_B(|\psi_i\rangle\langle\psi_i|)$ , i.e., the reduced density operator of subsystem  $A$ , and similarly for  $\rho_B$ . Entanglement of formation of  $\rho$  is then

$$E(\rho) := \min \sum_i p_i E(\psi_i), \quad (2.16)$$

where the minimization is taken over all pure-state decompositions of  $\rho$ . To derive an explicit analytic formula for  $E$ , Wootters defines *concurrence*, another measure of entanglement, as

$$C(\psi) := |\langle\psi|\tilde{\sigma}_y|\psi^*\rangle|, \quad (2.17)$$

where  $\tilde{\sigma}_y$  is the conventional Pauli spin matrix  $\sigma_y$ , if  $|\psi\rangle$  is a single-qubit state, and  $\sigma_y^{\otimes n}$ , if  $|\psi\rangle$  is an  $n$ -qubit state.

It holds that  $E(\psi) = \mathcal{E}[C(\psi)]$ , where the function  $\mathcal{E}$  is given by

$$\mathcal{E}(C) = H_{\text{bin}}\left(\frac{1 + \sqrt{1 - C^2}}{2}\right). \quad (2.18)$$

It is shown in Ref. [26] that

$$E(\rho) = \mathcal{E}[C(\rho)], \quad (2.19)$$

where

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \quad (2.20)$$

where the  $\lambda_i$  are the eigenvalues, in decreasing order, of a hermitian matrix  $R := \sqrt{\sqrt{\rho} \tilde{\rho} \sqrt{\rho}}$ , where tilde denotes the operation of complex conjugation followed by the operation of  $\tilde{\sigma}_y$ . Both  $E(\rho)$  and  $C(\rho)$  range from 0 to 1, and are zero for unentangled states and 1 for maximally entangled states, as is desirable for a measure of entanglement.

## 2.6 Quantum measurement

To fully specify an arbitrary state of a qubit, an infinite amount of information, in general, is needed: One has to announce the precise values of the complex numbers  $\alpha$  and  $\beta$  in Eq. (2.13). However, due to the nature of quantum measurements, only a finite amount of information can ever be extracted from a qubit. Hence, the exact values of  $\alpha$  and  $\beta$  of an unknown qubit state can never be learned with certainty.

The formalism of quantum measurements defines how much information can be gained on an array of qubits, with a specific measurement scheme. It should be noted that, in quantum mechanics, measurements are the only way of acquiring knowledge on a previously unknown physical system. In the course of our analysis, we employ two kinds of measurements: *projective* and *positive operator-valued measure* (POVM) measurements.

### 2.6.1 Projective measurements

Projective measurements are described in any reasonable introduction to quantum mechanics. Therefore, only a short definition is presented here. A projective measurement has a corresponding observable  $M$ , which has a decomposition

$$M = \sum_m m P_m , \quad (2.21)$$

where  $\{P_m\}$  are orthogonal projection operators to the eigenspaces with respective eigenvalues  $\{m\}$ . The eigenvalues are the possible outcomes upon measuring the observable  $M$ . If a state  $|\psi\rangle$  is measured, the probability of outcome  $m$  is

$$p(m) = \langle \psi | P_m | \psi \rangle . \quad (2.22)$$

Immediately after the measurement yielding  $m$ , the state of the system collapses to

$$\frac{P_m |\psi\rangle}{\sqrt{p(m)}} . \quad (2.23)$$

### 2.6.2 Positive operator-valued measures

Projective measurements are in general suitable for situations where there is interest in the evolution of the quantum system after the measurement. The converse is true for the POVM formalism which is more general than that of projective measurements, but still well suited for describing the probabilities of different outcomes.

Suppose there is a set of positive operators<sup>4</sup>  $\{E_m\}$  such that

$$\sum_m E_m = I . \quad (2.24)$$

Then the set  $\{E_m\}$  is a POVM, and the operators  $E_m$  are known as the corresponding *POVM elements*. The measurement that the POVM describes yields outcome  $m$  for state  $|\psi\rangle$  with probability

$$p(m) = \langle\psi|E_m|\psi\rangle . \quad (2.25)$$

For example, any projective measurement can be described with a POVM: The POVM elements are the projectors of the projective measurement,  $E_m = P_m$ . In general however, POVM elements need not be projectors. Hence, POVMs clearly describe a larger class of measurements than projective measurements alone.

Another example, adopted from Ref. [24], presents a measurement scheme with which one can possibly distinguish between states  $|\varphi_1\rangle = |0\rangle$  and  $|\varphi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ , and never make an error of identifying state  $|\varphi_1\rangle$  as  $|\varphi_2\rangle$ , or vice versa. Note that this characteristic cannot be achieved using only projective measurements. The POVM implementing this measurement scheme is

$$E_1 = \frac{\sqrt{2}}{1 + \sqrt{2}} |1\rangle\langle 1| , \quad (2.26)$$

$$E_2 = \frac{\sqrt{2}}{2(1 + \sqrt{2})} (|0\rangle - |1\rangle)(\langle 0| - \langle 1|) , \quad (2.27)$$

$$E_3 = I - E_1 - E_2 . \quad (2.28)$$

Now, suppose we measure a given state using the POVM  $\{E_1, E_2, E_3\}$ , knowing that the state is either  $|\varphi_1\rangle$  or  $|\varphi_2\rangle$ . If the measurement yields 1, we know that the given state was  $|\varphi_2\rangle$ . Similarly, result 2 implies that the state was  $|\varphi_1\rangle$ .

---

<sup>4</sup>A positive operator  $A: \mathcal{H} \rightarrow \mathcal{H}$  is such that  $\langle v|A|v\rangle$  is real and non-negative for any  $|v\rangle \in \mathcal{H}$ .



## 2.7 Quantum cloning

### 2.7.1 The no-cloning theorem

Unlike classical information, quantum information, in general, cannot be copied perfectly. This is due to the no-cloning property of quantum mechanics, stated as the *no-cloning theorem*: It is not possible to produce perfect copies of an unknown quantum state. Applied to qubits, the theorem states that given a qubit in state  $|Q\rangle = \alpha|0\rangle + \beta|1\rangle$ , we cannot produce the state  $|Q\rangle \otimes |Q\rangle$  without knowing the values of  $\alpha$  and  $\beta$ . The theorem does not state that we cannot produce a number of similar states  $|\Psi\rangle = |\psi\rangle \otimes |\psi\rangle \otimes \cdots \otimes |\psi\rangle$ , only that given a system in state  $|\psi\rangle$  with no additional information, we cannot create state  $|\Psi\rangle$ .

Let us give an elementary proof of the theorem, using *reductio ad absurdum*. The evolution of any quantum system can be described as unitary by appending an auxiliary system, or *ancilla*, to the original system. Now, suppose that a flawless copier exists. The copier has two slots, labelled  $S_1$  and  $S_2$ , and an ancilla. The ancilla may be of any dimension. Slot  $S_1$  occupies state  $|\psi\rangle$  representing the source, i.e., the state we wish to reproduce. Slot  $S_2$  is the target slot, which is to occupy the source state  $|\psi\rangle$  after the copying process. Slot  $S_2$  starts out in some initial state, denoted by  $|s_0\rangle$ . The initial state of the ancilla is  $|\mathcal{A}_0\rangle$ . That is, the initial state of the copying machine is

$$|\psi\rangle \otimes |s_0\rangle \otimes |\mathcal{A}_0\rangle . \quad (2.29)$$

The copying process, which can be assumed unitary, and is also assumed to leave the source and target states and the ancilla unentangled, is denoted by  $U_c$ , and it clones the state in  $S_1$  as [27]

$$U_c(|\psi\rangle|s_0\rangle|\mathcal{A}_0\rangle) = |\psi\rangle|\psi\rangle|\mathcal{A}_\psi\rangle . \quad (2.30)$$

The ancilla is left in state  $|\mathcal{A}_\psi\rangle$  that possibly depends on  $|\psi\rangle$ . The same must hold for copying the state  $|\phi\rangle \neq |\psi\rangle$ :

$$U_c(|\phi\rangle|s_0\rangle|\mathcal{A}_0\rangle) = |\phi\rangle|\phi\rangle|\mathcal{A}_\phi\rangle , \quad (2.31)$$

and for the superposition state  $|\Sigma\rangle = \frac{1}{\sqrt{2}}(|\phi\rangle + |\psi\rangle)$ :

$$\begin{aligned} U_c(|\Sigma\rangle|s_0\rangle|\mathcal{A}_0\rangle) &= |\Sigma\rangle|\Sigma\rangle|\mathcal{A}_\Sigma\rangle \\ &= \frac{1}{2}(|\phi\rangle + |\psi\rangle)(|\phi\rangle + |\psi\rangle)|\mathcal{A}_\Sigma\rangle \\ &= \frac{1}{2}(|\phi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle + |\psi\rangle|\psi\rangle)|\mathcal{A}_\Sigma\rangle . \end{aligned} \quad (2.32)$$

But because of linearity of quantum mechanics

$$\begin{aligned} U_c(|\Sigma\rangle|s_0\rangle|\mathcal{A}_0\rangle) &= \frac{1}{\sqrt{2}}(U_c(|\phi\rangle|s_0\rangle|\mathcal{A}_0\rangle) + U_c(|\psi\rangle|s_0\rangle|\mathcal{A}_0\rangle)) \\ &= \frac{1}{\sqrt{2}}(|\phi\rangle|\phi\rangle|\mathcal{A}_\phi\rangle + |\psi\rangle|\psi\rangle|\mathcal{A}_\psi\rangle) , \end{aligned} \quad (2.33)$$

which is clearly not compatible with Eq. (2.32), even if there were no ancilla in the copier. Hence, the assumption of the existence of a perfect cloning machine must be false.

### 2.7.2 Optimal cloning

We have shown that perfect cloning of quantum states is not possible. However, one can produce imperfect copies that are close to the original state with respect to some measure of cloning quality. Let us summarize the results on best possible discrete-system quantum cloning presented in Ref. [27]. Scarani *et al.* define  $N \rightarrow M$  cloning of pure states as

$$(|\psi\rangle^{\otimes N}) \otimes (|s_0\rangle^{\otimes (M-N)}) \otimes |\mathcal{A}_0\rangle \xrightarrow{U} |\Psi\rangle \quad (2.34)$$

where we continue the use of notation presented in Sec. 2.7.1, and  $U$  is the unitary cloning process. The quality of the produced copies is measured as *fidelity*  $F$ , which is defined

$$F_j := \langle \psi | \rho_j | \psi \rangle , \quad j \in \{1, \dots, M\} , \quad (2.35)$$

where  $\rho_j$  is the density operator of the partial state of clone  $j$  in  $|\Psi\rangle$ . For a *universal* copier,  $F_j$  is independent of the source state  $|\psi\rangle$ . For a *symmetric* copier,  $F_j$  is independent of  $j$ . A copier is *optimal* if it produces copies with maximal fidelity allowed by quantum physics, for a given source-state fidelity. The fidelity to be

maximized can be the average fidelity  $\bar{F} := \int_{\mathcal{S}} d\psi F(\psi)$ , or the minimum of fidelities  $F_{min} := \min_{\psi \in \mathcal{S}} F(\psi)$ , where  $\mathcal{S}$  is the set of source states.

The first quantum copying machine was presented by V. Bužek and M. Hillery in 1996 [28]. Their quantum copier is a universal, symmetric, optimal  $1 \rightarrow 2$  copier capable of duplicating a qubit, and achieving a fidelity of  $\frac{5}{6}$ . This generalizes to the universal, symmetric, optimal  $N \rightarrow M$  cloner for systems of any dimension  $d$  (not only for qubits, where  $d = 2$ ), whose fidelity is

$$F_d^{N \rightarrow M} = \frac{N}{M} + \frac{(M - N)(N + 1)}{M(N + d)}, \quad (2.36)$$

a result by R. F. Werner [29].

In asymmetric cloning, the produced copies have different fidelities. For example, the universal, asymmetric, optimal  $1 \rightarrow 2$  qubit-copying machine produces copies  $A$  and  $B$ , whose fidelities are

$$F_A = 1 - \frac{b^2}{2} \quad \text{and} \quad F_B = 1 - \frac{a^2}{2}, \quad (2.37)$$

where the real parameters  $a$  and  $b$  satisfy  $a^2 + b^2 + ab = 1$ . This result was found independently by several groups [27, 30, 31].

Again, the above mentioned qubit copier generalizes to the universal, asymmetric, optimal  $1 \rightarrow 2$  cloner capable of copying systems of dimension  $d$ , described in Refs. [32, 33]. Optimality was, however, proven later [34, 35]. The fidelities of the output systems of the cloner are

$$F_A = 1 - \frac{d-1}{d}b^2 \quad \text{and} \quad F_B = 1 - \frac{d-1}{d}a^2, \quad (2.38)$$

where the real parameters  $a$  and  $b$  now satisfy  $a^2 + b^2 + \frac{ab}{d} = 1$ .

Finally, we review the fidelity of a non-universal, i.e., state-dependent,  $1 \rightarrow 2$  qubit cloner, which is in addition *phase covariant*. In this context, phase covariance means that the cloner can clone, at best, states of the form

$$|\Psi(\varphi)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle). \quad (2.39)$$

The cloner, discussed in Ref. [36], transforms input states as

$$\begin{aligned} |0\rangle|0\rangle &\rightarrow |0\rangle|0\rangle \\ |1\rangle|0\rangle &\rightarrow \cos(\eta)|1\rangle|0\rangle + \sin(\eta)|0\rangle|1\rangle, \end{aligned} \quad (2.40)$$

where  $\eta \in [0, \frac{\pi}{2}]$ . Applying this to the state in Eq. (2.39) yields

$$|\Psi(\varphi)\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + \cos(\eta)e^{i\varphi}|1\rangle|0\rangle + \sin(\eta)e^{i\varphi}|0\rangle|1\rangle), \quad (2.41)$$

from which one obtains the fidelities

$$F_A = \frac{1}{2}(1 + \cos \eta) \quad \text{and} \quad F_B = \frac{1}{2}(1 + \sin \eta). \quad (2.42)$$

Note that these fidelities are independent of the phase factor  $\varphi$ .

## Chapter 3

# Quantum Key Distribution

Quantum key distribution (QKD) refers to any scheme that allows two distant parties to securely establish a shared, secret string of bits, and in which the security is based on the laws of quantum physics. C. H. Bennett and G. Brassard were the first to propose a practical protocol for QKD [7], known as the BB84 protocol. Section 3.1 describes the protocol in detail. The first experimental realization of the protocol is described in Ref. [14]. During the last two decades, the scientific community has introduced an overwhelming amount of modifications to the BB84 protocol, as well as entirely new QKD protocols [8–13, 37–61]. Some of these are briefly reviewed in Sec. 3.2.

Let us introduce the customary terminology of quantum cryptography. The initiator of the communication is *Alice*, and the party to whom Alice wants to send her messages is *Bob*. The all-purpose malevolent party who wishes to spy on Alice’s and Bob’s communication is *Eve*, the eavesdropper. If Alice or Bob co-operate with a non-malicious third party, he is called *Charlie*. A *channel* allows Alice and Bob to send data to each other. A channel can be one-way or two-way. A *classical channel* transmits bits, and a *quantum channel* transmits qubits. A *public channel* is one that anyone can listen to and to which anyone can send messages. If Alice and Bob use an *authenticated channel*, Eve cannot send messages such that they would appear to Bob to be from Alice, or vice versa. When considering the security of a particular cryptographic scheme, Eve is granted various capabilities. The set of Eve’s capabilities together with her actions during the execution of a protocol de-

finishes an *attack*. Section 3.1.5 describes attacks against the BB84 protocol. Section 3.2 summarizes attacks against other protocols.

## 3.1 BB84 protocol

Figure 3.1 shows a schematic illustration of the BB84 protocol. Alice and Bob are in possession of a two-way public authenticated classical channel. They also have a one-way public quantum channel, which allows Alice to send individual qubits to Bob. Eve is allowed total control of the quantum channel. That is, she can delete and insert transmissions, as well as alter them in any way that is not forbidden by the laws of quantum mechanics. Eve's interaction with the channel is denoted by  $E$ . In addition, Eve is assumed to listen in on every transmission on the classical channel. In the following description, we first assume no participation on Eve's behalf, and postpone the discussion of the effects introduced by Eve's interference to Sec. 3.1.5. Likewise, the discussion of an imperfect quantum channel is postponed to Sec. 3.1.4, and for now, both channels are assumed ideal, i.e., error-free. There is no Charlie in this protocol, that is, Alice and Bob do not have to rely on any third party to complete the key distribution.

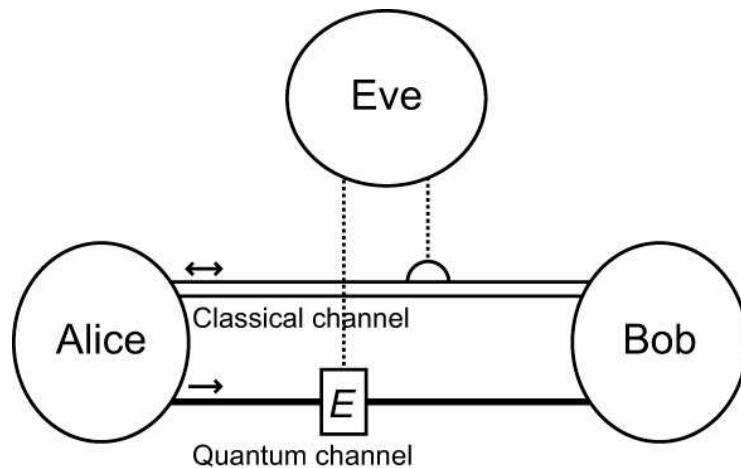


Figure 3.1: Setup of the BB84 quantum key distribution protocol. Alice and Bob use a two-way classical channel and a one-way quantum channel. Eve has total control over the quantum channel, whereas she can only listen to the classical channel.

### 3.1.1 Transmission

When Alice and Bob have decided, e.g., using the classical channel, to initiate the protocol, Alice begins the transmission of individual particles on the quantum channel. In the original paper, these particles are photons [7], and hence we will describe the protocol with photon transmission. However, any quantum system qualifying as a flying qubit<sup>1</sup> with two maximally conjugate bases would serve. Each of Alice's photons randomly occupy one of four possible states. Each state corresponds to a direction of linear polarization of the photon.

The choice of the state of each photon can be considered to consist of two binary random variables. The actual physical systems corresponding to these random variables are in Alice's possession. The first random variable  $A'$  represents the candidate for the bit value that Alice is trying to send to Bob. It is essential that  $p(A' = 0) = p(A' = 1) = \frac{1}{2}$ . Alice records for herself the outcomes of  $A'$ . The second random variable  $P_A$  determines in which basis the output of  $A'$  is transmitted. For  $P_A$  as well, we have to have  $p(P_A = z) = p(P_A = x) = \frac{1}{2}$ .

If  $P_A = z$ , Alice encodes the outcome 0 of  $A'$  as vertical polarization of the photon, and the outcome 1 as horizontal polarization of the photon. The vertical and horizontal polarization states are denoted by  $|\uparrow\rangle$  and  $|\leftrightarrow\rangle$ , respectively. Photons transmitted in either of these states are said to be sent in the  $\oplus$  basis. If  $P_A = x$ , Alice uses a diagonal basis: The outcome 0 of  $A'$  is encoded as the  $45^\circ$  rotated linear polarization, vertical being the non-rotated direction of polarization, and the outcome 1 of  $A'$  as the  $135^\circ$  rotated linear polarization. The respective states are denoted by  $|\nearrow\rangle$  and  $|\searrow\rangle$ . This is known as the  $\otimes$  basis.

The photon transmission states and bases can be equivalently described using the spin formalism of quantum mechanics. If  $P_A = z$ , Alice transmits in the eigenbasis of the Pauli spin matrix  $\sigma_z$ : The outcome 0 of  $A'$  is sent as  $|0\rangle$ , or equivalently as the spin-up state  $|\uparrow\rangle$ , and the outcome 1 as  $|1\rangle$ , equivalent to the spin-down state  $|\downarrow\rangle$ . If  $P_A = x$ , Alice transmits in the eigenbasis of the Pauli spin matrix  $\sigma_x$ : The outcome 0 of  $A'$  is sent as  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ , and the outcome 1 as  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ . In summary,  $|0\rangle = |\uparrow\rangle$ ,  $|1\rangle = |\leftrightarrow\rangle$ ,  $|+\rangle = |\nearrow\rangle$ ,  $|-\rangle = |\searrow\rangle$ , and basis  $\oplus$  corresponds

---

<sup>1</sup>See Sec. 2.4.1.

to the  $\sigma_z$  eigenbasis and basis  $\otimes$  to the  $\sigma_x$  eigenbasis—hence the labels  $z$  and  $x$  for the outcomes of  $P_A$ . The  $z$  and  $x$  bases are maximally conjugate in the sense that for any pair of states chosen from different bases, the square modulus of the inner product is  $|\langle 0|+\rangle|^2 = |\langle 0|-\rangle|^2 = \dots = \frac{1}{2}$ .

### 3.1.2 Measurement

Upon reception, Bob measures the polarization of each arriving photon. Bob's particular measurement is defined by a random variable  $P_B$ , whose physical system Bob is in total control of. The random variable  $P_B$  is identical to  $P_A$  in the sense that  $p(P_B = z) = p(P_B = x) = \frac{1}{2}$  but totally independent of  $P_A$ . If  $P_A$  and  $P_B$  were to depend on each other in some way, Alice and Bob would have to exchange information as  $P_A$  and  $P_B$  assume their values. This cannot be allowed, as it would severely compromise the security of the protocol. Therefore, it is required that  $P_A$  and  $P_B$  are independent.

Bob chooses the basis for his measurement of the direction of polarization in the same way that Alice chooses her basis of transmission. If  $P_B = z$ , Bob measures in  $\sigma_z$  eigenbasis, and if  $P_B = x$ , he measures in  $\sigma_x$  eigenbasis. Bob uses a projective measurement for each basis choice. For the  $z$  basis, the measurement projectors are  $P_0^z = |0\rangle\langle 0|$  and  $P_1^z = |1\rangle\langle 1|$ . For the  $x$  basis, Bob uses  $P_0^x = |+\rangle\langle +|$  and  $P_1^x = |-\rangle\langle -|$ . For example, in the  $x$  basis, when  $A' = 0$ , Bob recovers this with probability

$$p(0) = \langle +|P_0^x|+\rangle = \langle +|+\rangle\langle +|+\rangle = |\langle +|+\rangle|^2 = 1. \quad (3.1)$$

We observe that whenever the bases chosen by Alice and Bob coincide, Bob exactly recovers the value of Alice's random variable  $A'$ . This happens with probability

$$\begin{aligned} & p(P_A = P_B = z \text{ OR } P_A = P_B = x) \\ &= p(P_A = z, P_B = z) + p(P_A = x, P_B = x) \\ &= p(P_A = z)p(P_B = z) + p(P_A = x)p(P_B = x) \\ &= \frac{1}{2}, \end{aligned} \quad (3.2)$$

where we have used Eq. (2.1), the fact that only one basis is defined for Alice and Bob at a time, and the independence of  $P_A$  and  $P_B$ .



From Eq. (3.2), it follows that Bob uses a basis incompatible with Alice's basis with probability  $\frac{1}{2}$ . When this happens, Bob cannot recover the value of  $A'$ . For instance, if Alice has transmitted  $|+\rangle$  and Bob measures this in the wrong basis,

$$p(0) = \langle + | P_0^z | + \rangle = \frac{1}{2} (\langle 0 | + \langle 1 |) | 0 \rangle \langle 0 | (| 0 \rangle + | 1 \rangle) = \frac{1}{2} \langle 0 | 0 \rangle = \frac{1}{2}. \quad (3.3)$$

In fact, the same probability is obtained for each result and for each photon state given that Bob chooses the wrong basis for his measurement. That is, when the bases are not compatible, Bob gets the two possible results with equal probability.

### 3.1.3 Basis reconciliation

After each measurement, Bob interprets results  $|0\rangle$  and  $|+\rangle$  as 0, and results  $|1\rangle$  and  $|-\rangle$  as 1, and records this interpretation for himself. Bob's sequence of interpretations from the individual polarization measurements is known as the *raw key*. Because Alice and Bob choose the same bases with probability  $\frac{1}{2}$ , in the limit of a long key, only half of the bits in Bob's raw key are definitely the same as the output of  $A'$  recorded by Alice. For the measurements where Alice's and Bob's bases do not coincide, the result is, by chance, correct half the time, so on average half of this half of the raw-key bits agree. Since this is as good as Bob having simply guessed the values without any measurement, these bits have no value in this protocol, and Bob should discard them.

To be able to decide which bits to discard, Bob sends the sequence of his basis choices, i.e., outcomes of  $P_B$ , to Alice through the classical channel. Alice replies, through the classical channel, with her basis choices, i.e., outcomes of  $P_A$ . This is called basis reconciliation: Alice and Bob compare their basis-choice sequences, and discard all the bits where Bob used the wrong basis. That is, Alice and Bob keep only those bits for which their bases happened to coincide. What is left is an error-free shared string of bits known as the *sifted key*. Thus the protocol has achieved its goal. Table 3.1 presents an example of the use of this protocol.

For later purposes, it is convenient to model also the result of Bob's measurement, given that he used the same basis as Alice, as a random variable. Thus the outcomes of this random variable  $B$  determine the bits in Bob's sifted key. We define a

Table 3.1: A brief example of the BB84 QKD protocol. This example assumes error-free channels and no interference by Eve. Alice sends the photons in the state determined by her key-candidate and transmission-basis random variables. Bob measures the state of the photons in a randomly chosen basis, shown on line 5, and records his results (line 6). After the photon transmission is complete, Alice and Bob compare their basis choices and discard the bits for which their bases did not match. The remaining bits are shown on line 8. Finally, Alice and Bob choose randomly which bits to compare publicly (line 9), in order to estimate the quantum bit error rate of the transmission, described in Sec. 3.1.4.

1	Transmission	1 <sup>st</sup>	2 <sup>nd</sup>	3 <sup>rd</sup>	4 <sup>th</sup>	5 <sup>th</sup>	6 <sup>th</sup>	7 <sup>th</sup>	8 <sup>th</sup>	9 <sup>th</sup>	10 <sup>th</sup>
2	$A'$	1	0	1	1	0	1	1	0	0	1
3	$P_A$	$z$	$x$	$x$	$z$	$z$	$z$	$x$	$z$	$x$	$z$
4	Alice sends	$ 1\rangle$	$ +\rangle$	$ -\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ -\rangle$	$ 0\rangle$	$ +\rangle$	$ 1\rangle$
5	$P_B$	$x$	$z$	$x$	$x$	$z$	$z$	$z$	$z$	$x$	$x$
6	Raw key	0	1	1	0	0	1	1	0	0	1
7	$P_A = P_B$	no	no	yes	no	yes	yes	no	yes	yes	no
8	Sifted key			1		0	1		0	0	
9	Error estim.			no		no	yes		no	yes	
10	Key			1		0			0		

similar random variable for Alice: Outcomes of random variable  $A$  determine the bit values in Alice's sifted key, i.e., in the bit sequence in Alice's possession after basis reconciliation. The outcomes of  $A$  are a subset of the outcomes of  $A'$ . Bob's random variable  $B$  is, of course, highly dependent on  $A$ . For now, we state

$$p(B = 0|A = 0) = p(B = 1|A = 1) = 1 \quad (3.4)$$

$$p(B = 0|A = 1) = p(B = 1|A = 0) = 0. \quad (3.5)$$

These equations cease to hold if the assumption of non-interfering Eve is relaxed, or if the quantum channel is allowed a finite error rate.

### 3.1.4 Issues introduced by non-ideal equipment

The technology Alice and Bob use to implement a QKD protocol is never perfect. This section reviews the most important implications of the use of non-ideal equipment for the BB84 protocol. Firstly, the quantum channel conveying quantum states

from Alice to Bob is not perfect. Alice's transmission may be totally lost, or its polarization may be randomly rotated by a small angle. A lossy quantum channel poses no fundamental problem for Alice and Bob, as they can agree that Alice uses the classical channel to tell Bob when she transmits, and that Bob tells Alice which transmissions were successfully received. A quantum channel that randomly rotates the polarization of the photons causes errors to the sifted key, which means that Eqs. (3.4) and (3.5) do not hold anymore. The probability that Bob's measurement yields an incorrect result, even if he uses the same basis as Alice, is coined *quantum bit error rate* (QBER). That is, assuming an error process independent of the direction of polarization,  $p(B = 0|A = 1) = p(B = 1|A = 0) = \text{QBER}$ . Alice and Bob can obtain an estimate of the QBER by publicly comparing the values of a fraction of their respective sifted keys. Subsequently, they have to discard the bits whose values have been announced in public. Table 3.1 presents an example of this step. Working BB84-based QKD schemes have been reported with a QBER ranging from 1.0% to 10.2% [16, 62–64]. Errors in the sifted key can be corrected using classical error correction procedures with communication over the classical channel, described in Sec. 2.3.

Secondly, Bob's detectors are imperfect: Sometimes a detector fails to register a photon, and sometimes it incorrectly reports to have received a photon when in reality no transmission was received. Reports of the latter type are known as *dark counts*. Both of these effects can be counteracted with the same technique that was used to deal with a lossy channel: Alice and Bob declare their transmissions and receptions over the classical channel. Subsequently, Alice discards bits lost in the quantum channel or Bob's detector, and Bob discards excess bits created by dark counts. The rare event where a photon sent by Alice was lost in the channel, but Bob still observes a reception because of a dark count, contributes to the QBER. For instance, the following figures have been observed achievable in QKD experiments. A. Muller *et al.* have implemented the original BB84 protocol using photon polarization, reporting a detector efficiency of 0.2% and a dark count rate of  $700 \text{ s}^{-1}$ , with  $1.1 \cdot 10^6 \text{ s}^{-1}$  transmission rate at Alice's end [16], T. Hirano *et al.* have implemented a BB84 variant with detector efficiencies near 80% [63], and L. P. Lamoureux *et al.* report a 10.5% detector efficiency in a quantum coin-tossing protocol [65].

There are also several technical issues affecting the security of an implementation. One of the most serious problems is due to the fact that the BB84 protocol assumes that Alice can send individual photons to Bob. In reality, however, reliably creating transmissions containing exactly one photon is very difficult. Usually, single-photon pulses for QKD are created with an attenuated laser, for which the number of photons per pulse is a Poisson-distributed random variable [17]. Thus some of the pulses do not contain a photon at all, and some pulses contain one, two, or even more photons. Pulses containing more than one photon compromise the security of the protocol, since Eve can mount a specific attack based on multi-photon transmissions [66]. Therefore, the probability of transmitting more than one photon per transmission should be very small. Consequently, the probability of transmitting at least one photon tends to be quite small, as well. In Ref. [17], A. Ekert *et al.* present the following figures: The usual source used in QKD emits, on average, 0.1 photons per pulse, and 5% of the pulses that contain at least one photon, contain more than one photon. The authors anticipate that these figures will improve as technology advances. For instance, B. Darquié *et al.* reported in 2005 an experiment with a triggered source emitting single right-circularly polarized<sup>2</sup> photons [67]. Pulses from this source contain one photon with probability 0.981, and two photons with probability 0.019.

The implementation of the quantum channel of the protocol, including the detectors of Alice and Bob, may offer Eve the possibility of a *trojan horse* attack. In this type of attack, for example, Eve sends pulses of light to the quantum channel and observes the pattern of light reflected back from Alice's and Bob's equipment [18]. This way, Eve can, in principle, acquire information on the bases used by Alice and Bob, on the last value of Alice's key candidate variable  $A$ , or on the result of Bob's last measurement. Secure measures exist to thwart the trojan horse attack [68].

### 3.1.5 Attacks

In this section, we discuss attacks on the ideal BB84 protocol. That is, we abide by the framework presented in Fig. 3.1 and assume that Alice and Bob have taken

---

<sup>2</sup>Circular as well as linear polarization states can be used directly in BB84 [18].

all necessary precautions to counteract any security threats introduced by non-ideal equipment. Furthermore, Eve does not have access to Alice's or Bob's office, e.g., she cannot use a telescope to watch Bob's display. To recapitulate, Eve can only:

- i) Freely tamper with the quantum channel.
- ii) Listen in on everything that is transmitted on the classical channel.

A characteristic feature of quantum key distribution schemes is that any known method of eavesdropping inevitably causes errors to the quantum transmission, increasing the QBER. The errors allow Alice and Bob to detect Eve's interference and to obtain an estimate on Eve's maximal information about the key. In BB84, the QBER is the only, albeit guaranteed, indicator of Eve's interference. As described in Sec. 3.1.4, an error estimate is obtained by publicly comparing random bits in the sifted key. The accuracy of the estimate can be made arbitrarily high by increasing the number of compared bit values. An example of the estimation is included in Table 3.1. Alice and Bob have no way of resolving which errors are due to an imperfect quantum channel and which are due to Eve's actions, and they therefore safely assume that the estimated QBER is in its entirety due to Eve. After all, Eve could have, in principle, replaced most of the noisy quantum channel with a less noisy one. Alice and Bob correct errors of either origin using a classical error correction protocol.

Considering what Eve should do to gain knowledge on Alice and Bob's key, perhaps the first tactics that would come to one's mind is that Eve would capture each of Alice's qubit transmissions, prepare a copy of each for herself, and send another copy to Bob. Note that Eve has to send something to Bob, to allow him to continue the protocol—otherwise the transmission would never result in a key. Eve could keep her copies intact until Alice and Bob publicly announce their basis choices, and measure each transmission in the correct basis. She would then obtain a flawless copy of the key that Alice and Bob established without them knowing of this at all. However, this is where quantum physics steps in: According to the no-cloning theorem (Sec. 2.7.1), Eve cannot make perfect copies of all the states transmitted in the protocol. Therefore, this type of attack is simply not possible. However, if

Eve settles for flawed copies, the attack is feasible and considerable. This imperfect cloning attack is equivalent to an *incoherent attack*, discussed below.

### Intercept-resend

In the intercept-resend (IR) attack, Eve individually intercepts each qubit sent by Alice, measures the qubit state, and resends to Bob a qubit in the state corresponding to her measurement result. Eve performs her measurements exactly like Bob: For each qubit, she chooses at random between the two measurement bases: eigenbasis of  $\sigma_z$  or eigenbasis of  $\sigma_x$ . Alternatively, Eve can use the same basis every time. This does not affect the analysis, since Alice always transmits in a randomly chosen basis. If Eve uses the  $z$  basis in a measurement, result 0 means that Eve sends  $|0\rangle$ , and result 1 that she sends  $|1\rangle$  to Bob. If Eve's measurement basis is  $x$ , she resends  $|+\rangle$  if the result is 0, and  $|-\rangle$  if the result is 1. Note that, on average, Eve inevitably chooses the wrong basis with probability  $\frac{1}{2}$ . Thus, Eve's interference increases the QBER, based on which Alice and Bob estimate Eve's maximal information on Alice's sifted key, i.e., the outcomes of the random variable  $A$ .

Let us calculate exactly how much information, on average, the IR attack maximally provides Eve as a function of QBER. To verify that Eve indeed chooses the wrong basis with probability half, consider the two cases: Eve uses the same basis every time, or Eve chooses her basis randomly and uniformly. In the first case, because Alice's transmission basis is half the time  $z$  and half the time  $x$ , either fixed basis leads to Eve's choice being wrong on average half the time. As for the second case, let  $P_E$  denote Eve's measurement basis:  $p(P_E = z) = p(P_E = x) = \frac{1}{2}$ . The probability that Eve's choice is compatible with Alice's is

$$\begin{aligned}
 & p(P_A = P_E = z \text{ OR } P_A = P_E = x) \\
 &= p(P_A = z, P_E = z) + p(P_A = x, P_E = x) \\
 &= p(P_A = z)p(P_E = z) + p(P_A = x)p(P_E = x) \\
 &= \frac{1}{2}, \tag{3.6}
 \end{aligned}$$

exactly like in Eq. (3.2), and thus the choice is wrong half the time. Of course, Eve could favor, say, the  $z$  basis so that  $p(P_E = z) = 1 - p(P_E = x) > \frac{1}{2}$ . This strategy

does not change the probability obtained above, since it is equivalent to using a fixed choice some of the time, and a random choice with uniform probabilities some of the time. The probability of choosing wrong is  $\frac{1}{2}$  for both and thus Eve cannot increase, or decrease, the probability of her basis being the same as Alice's basis.

The knowledge that Eve has on Alice's bit sequence after basis reconciliation, i.e., outcomes of  $A$ , is quantified as the mutual information  $I(A, E)$ , where  $E$  is a random variable denoting the outcome of each of Eve's measurements. However,  $E$  only models measurements which correspond to transmissions that contribute to the sifted key. This is sensible because the basis reconciliation phase is public and thus Eve knows which bits Alice and Bob discard. According to Eq. (2.11),

$$I(A, E) = H(A) + H(E) - H(A, E) . \quad (3.7)$$

The entropy of Alice's random variable  $A$  is

$$H(A) = - \sum_{a=0}^1 p(a) \log p(a) = H_{\text{bin}}\left(\frac{1}{2}\right) = 1 . \quad (3.8)$$

To be able to express  $H(E)$ , we need to calculate the probability distribution of  $E$ , i.e., values  $p(E = 0)$  and  $p(E = 1)$ . Since  $p(E = 1) = 1 - p(E = 0)$ , it is sufficient to determine  $p(E = 0)$ . Eve can obtain the result  $E = 0$  in two mutually exclusive cases: Eve has the wrong basis, or Eve has the correct basis, compared to Alice's basis. Let  $B_w$  and  $B_c$  denote these events, respectively. In accordance with the law of total probability, Eq. (2.4), we have

$$\begin{aligned} p(E = 0) &= p(E = 0|B_w)p(B_w) + p(E = 0|B_c)p(B_c) \\ &= \frac{1}{2} [p(E = 0|B_w) + p(E = 0|B_c)] . \end{aligned} \quad (3.9)$$

The case where Eve chooses the correct basis is straightforward to analyze: Alice's transmission is in a state that already lies in the subspace of Eve's measurement projectors. For example,

$$p(E = 0, P_E = x | A = 0, P_A = x) = \langle + | P_0^x | + \rangle = \langle + | + \rangle \langle + | + \rangle = 1 . \quad (3.10)$$

Hence, Eve always correctly obtains the outcome of  $A$ , and we get

$$\begin{aligned}
p(E = 0|B_c) &\stackrel{(2.5)}{=} \sum_a p(E = 0, a|B_c) \\
&\stackrel{(2.6)}{=} \sum_a p(E = 0|a, B_c)p(a|B_c) \\
&= \sum_a p(E = 0|a, B_c)p(a) \\
&= \frac{1}{2} [p(E = 0|A = 0, B_c) + p(E = 0|A = 1, B_c)] \\
&= \frac{1}{2} (1 + 0) \\
&= \frac{1}{2}, \tag{3.11}
\end{aligned}$$

where  $a$  is the outcome of  $A$ , and we have used the fact that Alice's and Eve's basis choices are independent of  $A$ .

As for Eve's wrong choice of basis, the incorrect choice can be made in exactly two ways: by choosing the  $z$  basis, or by choosing the  $x$  basis. Furthermore, in each of these cases, Alice may have sent either 0 or 1. These four cases each yield probability  $\frac{1}{2}$  for  $E = 0$ , which can be observed by calculating

$$p(E = 0, P_E = z|A = 0, P_A = x) = \langle +|P_0^z|+ \rangle = \langle +|0 \rangle \langle 0|+ \rangle = |\langle +|0 \rangle|^2 = \frac{1}{2} \tag{3.12}$$

$$p(E = 0, P_E = x|A = 0, P_A = z) = \langle 0|P_0^x|0 \rangle = \langle 0|+ \rangle \langle +|0 \rangle = |\langle +|0 \rangle|^2 = \frac{1}{2}, \tag{3.13}$$

and similarly for the cases where  $A = 1$ . Thus,  $p(E = 0|B_w) = \frac{1}{2}$ , and we have  $p(E = 0) = p(E = 1) = \frac{1}{2}$  or in short  $p(e) = \frac{1}{2}$ , from which we finally obtain the entropy of Eve's measurement outcome

$$H(E) = - \sum_{e=0}^1 p(e) \log p(e) = H_{\text{bin}}\left(\frac{1}{2}\right) = 1. \tag{3.14}$$

To calculate the third term in Eq. (3.7),  $H(A, E)$ , we treat the cases of correct and incorrect basis separately, and use their average as the joint entropy  $H(A, E)$ . The use of an average is justified by noting that all the quantities related to Eve's



knowledge about the key are averaged over a large set of transmissions from Alice to Bob. That is, we are dealing with probabilities. Using the definitions of joint entropy, Eq. (2.10), and conditional probability, Eq. (2.2), we expand

$$\begin{aligned}
H(A, E) &= - \sum_{a,e} p(a, e) \log p(a, e) \\
&= - \sum_{a,e} p(e|a)p(a) \log[p(e|a)p(a)] \\
&= - \frac{1}{2} \sum_{a,e} p(e|a) \log \left[ \frac{1}{2} p(e|a) \right] \\
&= \frac{1}{2} \sum_{a,e} p(e|a) - \frac{1}{2} \sum_{a,e} p(e|a) \log p(e|a) . \tag{3.15}
\end{aligned}$$

We have already calculated the probabilities  $p(e|a)$ . If Eve chooses her basis correctly,  $p(0|0) = p(1|1) = 1$  and  $p(0|1) = p(1|0) = 0$ . Thus the joint entropy in the case of correct basis is 1. When Eve chooses the wrong basis,  $p(0|0) = p(0|1) = p(1|0) = p(1|1) = \frac{1}{2}$ . Thus the joint entropy for an incorrect basis choice is 2. Because Eve's basis choice is correct on average half the time,  $H(A, E) = \frac{3}{2}$ . Applying the results to Eq. (3.7) gives  $I(A, E) = \frac{1}{2}$ . That is, Eve gains 0.5 bits of information per bit in the sifted key.

The results are very intuitive. When Eve's basis is correct,  $E$  gives exactly the same information as  $A$  without error. When Eve's basis is incorrect, she gets results that are totally random, and  $E$  conveys no information on  $A$ . The correct basis is used with probability  $\frac{1}{2}$ , i.e., half the time in a large set of interceptions. Therefore, Eve gets half of the bits in Alice's sifted key, and the rest is random noise.

There is an alternative and somewhat simpler formulation for Eve's knowledge on the sifted key, which we will later use in our analysis. One defines a composite random variable  $\tilde{A}$  for the joint outcome of  $A$  and  $P_A$ . That is,  $\tilde{A}$  describes the quantum state of Alice's transmission, and assumes its values  $\tilde{a}$  from the set  $\{0, 1, +, -\}$  with uniform probability  $p(\tilde{a}) = \frac{1}{4}$ . In the following, we prove that calculating Eve's information on the transmission state  $\tilde{A}$  yields exactly the same result as calculating her information on  $A$ , i.e.,  $I(\tilde{A}, E) = I(A, E)$ .

The mutual information of  $\tilde{A}$  and  $E$  is

$$I(\tilde{A}, E) = H(\tilde{A}) + H(E) - H(\tilde{A}, E) , \tag{3.16}$$

where  $H(E) = 1$ , as before, and

$$\begin{aligned}
 H(\tilde{A}) &= - \sum_{\tilde{a}=0}^{-} p(\tilde{a}) \log p(\tilde{a}) \\
 &= - \sum_{\tilde{a}=0}^1 p(\tilde{a}) \log p(\tilde{a}) - \sum_{\tilde{a}=+}^{-} p(\tilde{a}) \log p(\tilde{a}) \\
 &= -2 \sum_{\tilde{a}=0}^1 p(\tilde{a}) \log p(\tilde{a}) .
 \end{aligned} \tag{3.17}$$

Noting that  $p(a) = 2p(\tilde{a})$  for  $a, \tilde{a} \in \{0, 1\}$ , we obtain

$$\begin{aligned}
 H(A) &= - \sum_{a=0}^1 p(a) \log p(a) \\
 &= -2 \sum_{\tilde{a}=0}^1 p(\tilde{a}) \log [2p(\tilde{a})] \\
 &= -2 \sum_{\tilde{a}=0}^1 p(\tilde{a}) - 2 \sum_{\tilde{a}=0}^1 p(\tilde{a}) \log p(\tilde{a}) \\
 &= -2 \sum_{\tilde{a}=0}^1 p(\tilde{a}) + H(\tilde{A}) .
 \end{aligned} \tag{3.18}$$

Now let us expand the joint entropy of  $\tilde{A}$  and  $E$  to ultimately show that the difference in the entropies of  $\tilde{A}$  and  $A$  is exactly cancelled by the same difference in the joint entropies. The joint entropy is the average of joint entropies of Eve's different basis choices,  $H_z(\tilde{A}, E)$  and  $H_x(\tilde{A}, E)$ , which are in fact equal. That is,

$$\begin{aligned}
 H(\tilde{A}, E) &= \frac{1}{2} H_z(\tilde{A}, E) + \frac{1}{2} H_x(\tilde{A}, E) \\
 &= -\frac{1}{2} \sum_{e=0}^1 \sum_{\tilde{a}=0}^{-} p(e|\tilde{a}, P_E = z) p(\tilde{a}) \log [p(e|\tilde{a}, P_E = z) p(\tilde{a})] \\
 &\quad -\frac{1}{2} \sum_{e=0}^1 \sum_{\tilde{a}=0}^{-} p(e|\tilde{a}, P_E = x) p(\tilde{a}) \log [p(e|\tilde{a}, P_E = x) p(\tilde{a})]
 \end{aligned}$$

$$\begin{aligned}
&= -\frac{1}{2} \sum_{e=0}^1 \sum_{\tilde{a}=0}^1 p(\tilde{a}) \{ [p(e|\tilde{a}, P_E = z) + p(e|\tilde{a}, P_E = x)] \log p(\tilde{a}) \\
&\quad + p(e|\tilde{a}, P_E = z) \log p(e|\tilde{a}, P_E = z) + p(e|\tilde{a}, P_E = x) \log p(e|\tilde{a}, P_E = x) \} \\
&\quad -\frac{1}{2} \sum_{e=0}^1 \sum_{\tilde{a}=+}^- p(\tilde{a}) \{ [p(e|\tilde{a}, P_E = z) + p(e|\tilde{a}, P_E = x)] \log p(\tilde{a}) \\
&\quad + p(e|\tilde{a}, P_E = z) \log p(e|\tilde{a}, P_E = z) + p(e|\tilde{a}, P_E = x) \log p(e|\tilde{a}, P_E = x) \} \\
&= -\frac{1}{2} \sum_{e=0}^1 \sum_{\tilde{a}=0}^1 p(\tilde{a}) \{ [p(e|\tilde{a}, B_c) + p(e|\tilde{a}, B_w)] \log p(\tilde{a}) \\
&\quad + p(e|\tilde{a}, B_c) \log p(e|\tilde{a}, B_c) + p(e|\tilde{a}, B_w) \log p(e|\tilde{a}, B_w) \} \\
&\quad -\frac{1}{2} \sum_{e=0}^1 \sum_{\tilde{a}=+}^- p(\tilde{a}) \{ [p(e|\tilde{a}, B_w) + p(e|\tilde{a}, B_c)] \log p(\tilde{a}) \\
&\quad + p(e|\tilde{a}, B_w) \log p(e|\tilde{a}, B_w) + p(e|\tilde{a}, B_c) \log p(e|\tilde{a}, B_c) \} \\
&= -\sum_{e=0}^1 \sum_{\tilde{a}=0}^1 p(\tilde{a}) \{ [p(e|\tilde{a}, B_c) + p(e|\tilde{a}, B_w)] \log p(\tilde{a}) \\
&\quad + p(e|\tilde{a}, B_c) \log p(e|\tilde{a}, B_c) + p(e|\tilde{a}, B_w) \log p(e|\tilde{a}, B_w) \} , \tag{3.19}
\end{aligned}$$

where we have used the fact that the  $z$  basis is correct for  $\tilde{a} = 0, 1$  and incorrect for  $\tilde{a} = +, -$ , and conversely for the  $x$  basis. The last equality follows from the equality of the sums over  $\tilde{a}$ .

For the joint entropy of  $A$  and  $E$  we use again the average over the cases of correct and incorrect measurement basis:

$$\begin{aligned}
H(A, E) &= \frac{1}{2} H_c(A, E) + \frac{1}{2} H_w(A, E) \\
&= -\frac{1}{2} \sum_{e=0}^1 \sum_{a=0}^1 p(e|a, B_c) p(a) \log [p(e|a, B_c) p(a)] \\
&\quad -\frac{1}{2} \sum_{e=0}^1 \sum_{a=0}^1 p(e|a, B_w) p(a) \log [p(e|a, B_w) p(a)] \\
&= -\frac{1}{2} \sum_{e=0}^1 \sum_{a=0}^1 p(a) \{ [p(e|a, B_c) + p(e|a, B_w)] \log p(a) \\
&\quad + p(e|a, B_c) \log p(e|a, B_c) + p(e|a, B_w) \log p(e|a, B_w) \}
\end{aligned}$$

$$\begin{aligned}
&= - \sum_{e=0}^1 \sum_{\tilde{a}=0}^1 p(\tilde{a}) \{ [p(e|\tilde{a}, B_c) + p(e|\tilde{a}, B_w)] \log(2p(\tilde{a})) \\
&\quad + p(e|\tilde{a}, B_c) \log p(e|\tilde{a}, B_c) + p(e|\tilde{a}, B_w) \log p(e|\tilde{a}, B_w) \} \\
&\stackrel{(3.19)}{=} - \sum_{e=0}^1 \sum_{\tilde{a}=0}^1 p(\tilde{a}) [p(e|\tilde{a}, B_c) + p(e|\tilde{a}, B_w)] + H(\tilde{A}, E) \\
&\stackrel{(2.4)}{=} - \sum_{e=0}^1 \sum_{\tilde{a}=0}^1 p(\tilde{a}) \cdot 2p(e|\tilde{a}) + H(\tilde{A}, E) \\
&\stackrel{(2.3)}{=} - 2 \sum_{\tilde{a}=0}^1 \sum_{e=0}^1 p(e)p(\tilde{a}|e) + H(\tilde{A}, E) \\
&\stackrel{(2.4)}{=} - 2 \sum_{\tilde{a}=0}^1 p(\tilde{a}) + H(\tilde{A}, E) . \tag{3.20}
\end{aligned}$$

Equations (3.16), (3.18), and (3.20) yield

$$\begin{aligned}
I(A, E) &= H(E) + H(A) - H(A, E) \\
&= H(E) - 2 \sum_{\tilde{a}=0}^1 p(\tilde{a}) + H(\tilde{A}) + 2 \sum_{\tilde{a}=0}^1 p(\tilde{a}) - H(\tilde{A}, E) \\
&= H(E) + H(\tilde{A}) - H(\tilde{A}, E) \\
&= I(\tilde{A}, E) , \tag{3.21}
\end{aligned}$$

which completes our proof. Note that in obtaining Eq. (3.21) we used only three assumptions:

- i)  $p(\tilde{A} = 0) = p(\tilde{A} = +)$  and  $p(\tilde{A} = 1) = p(\tilde{A} = -)$ .
- ii)  $p(a) = 2p(\tilde{a})$  for  $a, \tilde{a} \in \{0, 1\}$ .
- iii) For  $\tilde{a} = 0, 1$ , the  $z$  basis is correct and the  $x$  basis incorrect, and vice versa for  $\tilde{a} = +, -$ .

Next, we analyze how much errors Eve's strategy induces to Bob's sifted key, i.e., we calculate the QBER that Alice and Bob observe, given that Eve uses the IR strategy. The error rate is defined as the probability that an individual bit value in Bob's sifted key differs from the corresponding value in Alice's sifted key. Formally,

$$\text{QBER} = p(b \neq a) = \sum_a p(B = \bar{a} | A = a) p(a) , \tag{3.22}$$

where  $a$  and  $b$  are the outcomes of Alice and Bob's random variables  $A$  and  $B$ , respectively. The bar over the symbol  $\bar{a}$  represents an increment of 1 modulo 2, i.e.,  $\bar{0} = 1$  and  $\bar{1} = 0$ . The reader is reminded that Eve is in total control of the states that Bob receives, but has only partial control over Bob's measurement results, i.e., outcomes of  $B$ .

Because we are considering bits in the sifted key only, the correctness of Bob's result depends on Eve's basis choice:

$$\begin{aligned}
 \text{QBER} &= \sum_a p(B = \bar{a} | A = a) p(a) \\
 &\stackrel{(2.5)}{=} \sum_a \underbrace{[p(B = \bar{a}, B_c | A = a) + p(B = \bar{a}, B_w | A = a)]}_{=0} p(a) \\
 &\stackrel{(2.6)}{=} \sum_a p(B = \bar{a} | B_w, A = a) p(B_w | A = a) p(a) \\
 &= \frac{1}{2} \sum_a p(B = \bar{a} | B_w, A = a) p(B_w) \\
 &= \frac{1}{4} \sum_{a=0}^1 p(B = \bar{a} | B_w, A = a) \\
 &= \frac{1}{4} \left( \frac{1}{2} + \frac{1}{2} \right) = \frac{1}{4}, \tag{3.23}
 \end{aligned}$$

where we have used the fact that when Eve's basis choice is wrong, i.e., incompatible with Alice's choice, it is also incompatible with Bob's choice, in which case Bob gets an incorrect result with probability  $\frac{1}{2}$ .

In summary, we have shown that the IR attack strategy gives Eve 0.5 bits of information per interception and induces an average QBER of 25% in the sifted key. In practice, a 25% QBER would probably be considered too high by Alice and Bob, and they would thus abort the protocol. However, Eve does not have to intercept every transmission, instead, she can choose to interfere with only a fraction  $0 \leq \xi \leq 1$  of the transmissions. Then Eve's information as well as the QBER is linearly parametrized by  $\xi$ :

$$I_{A,E}(\xi) = \xi/2, \tag{3.24}$$

$$\text{QBER}(\xi) = \xi/4, \tag{3.25}$$

from which the maximal information Eve can gain for a given QBER  $q$  is

$$I_{max}^{\text{IR}}(q) = \begin{cases} 2q & \text{if } 0 \leq q \leq 1/4 \\ 0.5 & \text{if } 1/4 < q \leq 1/2. \end{cases} \quad (3.26)$$

### Incoherent attack

In an incoherent or individual attack, Eve entangles each transmitted qubit individually to a *probe*. Eve's probes are quantum systems capable of retaining their state until the basis reconciliation phase. Alternatively, the state of each probe can be kept in separate quantum memory<sup>3</sup>. The probes are assumed to be identical, and there is one probe for each eavesdropped transmission. Four-dimensional, i.e., two-qubit, probes are sufficient for Eve's purposes in BB84 [71]. After basis reconciliation, Eve measures the probe states one-by-one in an attempt to gain as much information as possible on the sifted key. The qubit-probe interaction  $\mathcal{U}$  can be assumed unitary<sup>4</sup> and independent of the state of the qubit. The interaction can be viewed as an act of transferring information from the transmitted qubit to one or more probe qubits. For Eve, the optimal choices of  $\mathcal{U}$  are parametrized by a real variable  $\eta$ . Therefore, variable  $\eta$  actually parametrizes a whole—uncountably infinite—family of attacks referred to as incoherent attacks.

The maximal mutual information that Eve can gain with an incoherent attack is

$$\begin{aligned} I_{max}^{\text{incoh.}}(q) = & \left( \frac{1}{2} + \sqrt{q(1-q)} \right) \log(1 + 2\sqrt{q(1-q)}) \\ & + \left( \frac{1}{2} - \sqrt{q(1-q)} \right) \log(1 - 2\sqrt{q(1-q)}) , \end{aligned} \quad (3.27)$$

where  $q$  is a given QBER. It is also known that an interaction  $\mathcal{U}$  and a probe measurement scheme achieving this bound exist [72].

An incoherent attack achieving the bound in Eq. (3.27) is equivalent to optimal cloning of the transmitted qubit. The optimal cloner is the  $1 \rightarrow 2$  phase-covariant qubit cloner defined by transformation (2.40), which is justified as follows. We

---

<sup>3</sup>Long-term quantum memory is a delicate issue in its own right. Photonic physical-qubit memories are discussed, for example, in Refs. [69, 70].

<sup>4</sup>A non-unitary interaction would be equivalent to a unitary one, only with a higher-dimensional probe.

only consider transmissions that contribute to the sifted key. We assume that Eve attempts to clone state  $|+\rangle$ , since the calculation is similar for all other BB84 states. Setting  $\varphi = 0$ , Eq. (2.41) yields the result of the cloning process as

$$|C\rangle = \mathcal{U}|+\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + \cos(\eta)|1\rangle|0\rangle + \sin(\eta)|0\rangle|1\rangle) . \quad (3.28)$$

Eve then sends Bob the qubit in the first slot and keeps the qubit in the second slot for herself. When Bob measures his qubit, he gets the correct result, i.e., zero in the  $x$  basis, with probability

$$p(B = 0) = \langle C|(P_0^x \otimes I)|C\rangle = \frac{1}{2}(1 + \cos \eta) . \quad (3.29)$$

Hence, the QBER is

$$q(\eta) = \frac{1}{2}(1 - \cos \eta) . \quad (3.30)$$

The best strategy for Eve is to simply measure her probe qubit the same way she measures transmitted qubits in the IR attack. However, because Eve can keep her probes intact until she learns which basis Alice has used in the transmission, she knows in which basis to perform the measurement. Eve gets the correct result in the  $x$  basis with probability

$$P_{E=0}(\eta) = \frac{1}{2}(1 + \sin \eta) . \quad (3.31)$$

Eve's mutual information on the key decreases with increasing uncertainty in her measurement result. That is,

$$I_{A,E}(\eta) = 1 - H_{\text{bin}}[P_{E=0}(\eta)] . \quad (3.32)$$

Eliminating  $\eta$  in Eqs. (3.30) and (3.32) yields the bound in Eq. (3.27). Note the equivalence of Eqs. (3.29), (3.31) and the fidelities given in Eq. (2.42). For a more detailed description of the cloning process, see Ref. [27].

Interacting with only a fraction  $\xi$  of the transmissions does not provide Eve any advantage. This is because the mutual-information bound in Eq. (3.27) is a concave function of  $q$ , and hence, for a fixed QBER, adjusting the parameter  $\eta$  and probing every transmission is always at least as beneficial as not probing every transmission. Figure 3.2 shows the maximal mutual information as a function of a given QBER for the incoherent and intercept-resend attacks.

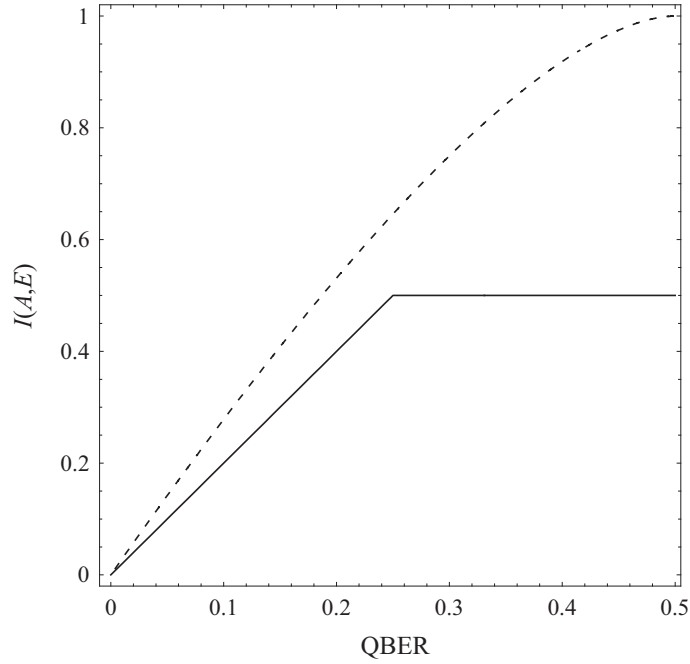


Figure 3.2: Eve’s maximal information on Alice’s sifted key for a given QBER for intercept-resend (solid line) and incoherent (dashed line) attack strategies against the BB84 protocol.

### Coherent attack

In a coherent attack, Eve is in possession of an unlimited-dimensional probe in an arbitrary initial state. Eve is allowed to apply any unitary transformation to the entire transmitted qubit sequence and the probe. The probe state is retained until all public discussions between Alice and Bob are finished, and Eve is then allowed to perform arbitrary measurements on the probe system as a whole. Collective attacks are a subclass of coherent attacks, in which Eve is allowed to entangle the qubits and probes individually but still use any conceivable measurement scheme after Alice and Bob’s public discussions. [17]

For coherent attacks, the various security proofs state that the probability, that Alice and Bob unknowingly agree on a key that Eve has more than an exponentially small amount of information, is exponentially small in some security parameter



under Alice and Bob's control. No explicit maximal mutual information for a given QBER has been presented in the literature. [68, 73–78]

### 3.1.6 Privacy amplification

Because an error-free quantum channel does not exist, Alice and Bob have to work with some finite QBER. Consequently, they can never be absolutely certain that Eve has not eavesdropped parts of the generated key. Given a long enough key sequence, however, Alice and Bob can shorten the key and reduce Eve's information on it to an arbitrarily low value by public classical communication. This procedure is called privacy amplification.

The essential step in privacy amplification algorithms is typically the following: Alice randomly chooses a pair of slots  $\{i, j\}$  in the error-corrected sifted key and informs Bob of her choice. Both participants then calculate  $c_{ij} = \text{XOR}(a_i, a_j)$ . Alice and Bob obtain the same value for  $c_{ij}$ , since their bit strings are identical. They then replace the bits in slots  $i$  and  $j$  with the value  $c_{ij}$ . Any uncertainty Eve has about the bit values in the slots is always increased by this process. For example, if Eve only knows the value of the bit in slot  $i$ , after privacy amplification she knows nothing of the value of slot  $i$ . This step is iterated for as long as is necessary to bring Eve's maximal information on the key to a low enough value. More sophisticated protocols work on larger bit blocks. [18]

## 3.2 Other protocols

### 3.2.1 Einstein-Podolsky-Rosen protocol

In 1991, A. Ekert published the Einstein-Podolsky-Rosen (EPR) QKD protocol, sometimes referred to as E91 [13]. This protocol is named after the famous EPR thought experiment constructed to prove that quantum mechanics is not a complete description of reality [24, 79]. In the EPR protocol, Alice and Bob do not send quantum states to each other, but instead rely on a third party, Charlie, to transmit two

qubits in an entangled state, one qubit to Alice and the other to Bob. Specifically, the state that Charlie emits is

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \quad (3.33)$$

also known as one of the Bell states. A pair of qubits in this state are said to form an *EPR pair*. Upon reception of the qubits, Alice and Bob randomly choose between two measurement bases, just as in BB84. Later the bases are announced in public, and the sifted key is obtained by discarding the results for which the bases did not match.

Alice and Bob can perform a test to see whether Charlie truly emits the state in Eq. (3.33). This test is based on Bell's inequality which demonstrates that a local theory cannot give the correlations that quantum mechanics predicts [80]. To be completely assured that Eve has not tampered with the emitted state, Alice and Bob must observe a maximal violation of Bell's inequality. In practice, because of noise or eavesdropping, only a sub-maximal violation is observed, requiring the use of error correction and privacy amplification for obtaining a secret key. When Charlie emits state  $|\Phi^+\rangle$ , this protocol is equivalent to BB84 [18].

### 3.2.2 Two-state protocol

In 1992, C. H. Bennett proposed a simple variant of the original BB84 protocol [8]. It is known as B92 or the two-state protocol. The latter name comes from the essential modification to BB84. The four states  $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$  used in BB84 are more than is necessary for Eve not being able to eavesdrop the transmissions without being noticed. In fact, using only two non-orthogonal states suffices, e.g.,  $|0\rangle$  and  $|+\rangle$ . In the B92 protocol, Alice randomly chooses which one of the two states she transmits, and Bob randomly chooses a measurement basis for each reception. The rest of the protocol is identical to BB84. The requirement of transmitting only two different states renders the experimental implementation of the protocol less demanding. Although Eve still inevitably perturbs the transmission if she interferes with it, she can unambiguously distinguish between the two states at the cost of some transmissions being lost completely. [18]

### 3.2.3 Six-state protocol

Another fairly simple variant of BB84 is the six-state protocol proposed by D. Bruß in 1998 [9]. The six-state protocol uses three conjugate bases for the quantum channel transmissions: not only the eigenbases of Pauli matrices  $\sigma_x$  and  $\sigma_z$  but also the eigenbase of  $\sigma_y$ . Alice randomly transmits and Bob randomly measures in one of these bases. The intercept-resend strategy induces a 33% QBER in this protocol. If Eve employs an incoherent attack against this protocol, then given a QBER  $q$ , her maximal information on the key is

$$I_{max}^{incoh.}(q) = 1 - (1 - q)H_{bin}[g(q)] , \text{ where} \quad (3.34)$$

$$g(q) = \frac{1}{2} \left( 1 + \frac{1}{1 - q} \sqrt{q(2 - 3q)} \right) . \quad (3.35)$$

This is less than, although close to, the maximum in Eq. (3.27) for  $0 < q < 0.5$ . That is, to achieve the same information on the key, Eve must induce a slightly higher QBER than in the original BB84. However, because Alice and Bob use three different bases, Bob chooses the correct basis on average only  $\frac{1}{3}$  of the time. Therefore, to generate a sifted key of given length, more quantum transmissions are needed than in the BB84 protocol.

### 3.2.4 Adjusted basis probabilities protocol

In the original BB84 protocol, the two transmission and measurement bases  $z$  and  $x$  are chosen with equal probabilities. In 1998, M. Ardehali *et al.* proposed a variant in which the use of one of the bases has a significantly higher probability [10]. The adjusted probability is announced in public. The advantage of this modification is that a considerably smaller amount of measurement results need to be discarded in the basis reconciliation phase. However, Eve's information on the key is higher, since she can always employ the basis that is used more frequently. To counteract this, the authors suggest a sophisticated error analysis scheme. It is not clear whether this modification ultimately improves on the efficiency of BB84.

# Chapter 4

## Analysis and Results

This chapter describes in detail our proposed amendment to the BB84 protocol. The purpose of the modification is to yield Alice and Bob advantage against an eavesdropper in terms of mutual information. As a demonstration of the idea behind the modification, we present an analysis of the difficulty of approximating an entangled state of two qubits with two product-state qubits. As our main result, we give explicit bounds on the information of an eavesdropper employing an intercept-resend attack against our protocol as a function of the qubit error rate. We also discuss a special kind of attack against this protocol, one in which Eve recreates destroyed entanglement using EPR pairs.

### 4.1 Proposed modification to the BB84 protocol

We analyze a protocol based on the BB84 protocol. Our protocol differs from the original one in the following:

1. Prior to the key distribution, Alice and Bob publicly agree on an  $N$ -qubit unitary transformation  $U: \mathcal{H}^N \rightarrow \mathcal{H}^N$ .
2. Alice's actions differ from BB84 such that she

- (a) postpones her transmissions<sup>1</sup> until she has generated  $N$  qubits to transmit,
  - (b) then applies  $U$  to the qubits, and
  - (c) transmits them one at a time, always waiting for Bob to acknowledge the reception of the previous qubit before sending the next one.
3. Bob's actions differ from BB84 such that he
- (a) postpones his measurements until  $N$  qubits have arrived,
  - (b) immediately acknowledges each received qubit to Alice, and
  - (c) having received a sequence of  $N$  qubits, applies  $U^{-1} = U^\dagger$  to the qubits and measures them exactly as in BB84.

The transformation  $U$  can be viewed as an extension or a plug-in to the BB84 protocol. Without Eve's interference, the use of  $U$  and  $U^{-1}$  is fully transparent from Alice's and Bob's point of view. Note that Eve is fully aware of  $U$ , since it is announced in public. Because Bob acknowledges every arrived qubit, Eve has only one-by-one access to the particles of the  $N$ -qubit state. The transformation is

$$U(|a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_N\rangle) = |\psi_{a_1, a_2, \dots, a_N}\rangle, \quad (4.1)$$

where  $|a_i\rangle$  are the states of the original BB84 protocol, i.e.,  $|a_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ . In our modified protocol, Alice sends the qubits of the state  $|\psi_{a_1, a_2, \dots, a_N}\rangle$  to Bob one at a time.

If  $U$  is of the form

$$U = U_1 \otimes U_2 \otimes \cdots \otimes U_N, \quad (4.2)$$

where  $U_j$  are single-qubit gates, i.e.,  $U_j: \mathbb{C}^2 \rightarrow \mathbb{C}^2$  for  $j \in \{1, 2, \dots, N\}$ , then

$$\begin{aligned} U(|a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_N\rangle) &= (U_1 \otimes U_2 \otimes \cdots \otimes U_N)(|a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_N\rangle) \\ &= U_1|a_1\rangle \otimes U_2|a_2\rangle \otimes \cdots \otimes U_N|a_N\rangle \\ &= |\psi_{a_1}\rangle \otimes |\psi_{a_2}\rangle \otimes \cdots \otimes |\psi_{a_N}\rangle. \end{aligned} \quad (4.3)$$

---

<sup>1</sup>Postponing the processing of existing qubits in items 2(a), 2(c), and 3(a) requires that Alice and Bob employ short-term quantum memory.

In other words, if  $U$  is decomposable to single-qubit gates, the transmitted  $N$ -qubit state is a product state. Given the product state, Eve can perfectly undo  $U$ , attack the individual unentangled qubits, and reconstruct the transmitted state by using the single-qubit gates  $U_j^\dagger$  and  $U_j$ . Therefore, Alice and Bob should choose  $U$  such that it produces an entangled  $N$ -qubit state. This implies

$$U \neq U_1 \otimes U_2 \otimes \cdots \otimes U_N . \quad (4.4)$$

That is, by using a non-local  $U$ , Alice and Bob utilize entanglement to prohibit Eve from fully accessing the transmitted qubits. In the following sections we restrict our analysis to the case  $N = 2$ .

## 4.2 Product-state approximation of an entangled qubit pair

To demonstrate the underlying idea in using an entangling  $N$ -qubit gate in BB84, we perform an analysis on how closely an entangled two-qubit state can be approximated with two product-state qubits. This analysis shows that even if perfect cloning of quantum states was possible, the protocol poses an inherent limitation for Eve.

Assume that Eve constructs the state

$$\bigotimes_{i=1}^N |\psi_i\rangle , \quad |\psi_i\rangle \in \mathbb{C}^2 = \mathcal{H}^1 , \quad |||\psi_i\rangle|| = 1 , \quad (4.5)$$

in an attempt to approximate a normalized state  $|\psi\rangle \in \mathbb{C}^{2^N} = \mathcal{H}^N$  being transmitted one qubit at a time from Alice to Bob. Eve tries to minimize the error in this approximation whereas Alice and Bob want to maximize Eve's minimal error by choosing  $|\psi\rangle$  appropriately. This maximal-minimal error is

$$E_{\text{mm}} := \max_{|\psi\rangle} \min_{\{|\psi_i\rangle\}} \left\| |\psi\rangle - \bigotimes_{i=1}^N |\psi_i\rangle \right\| . \quad (4.6)$$

### 4.2.1 Theory

We assume that Alice and Bob have chosen  $N = 2$ . We write the state Alice uses as

$$|\psi\rangle = \begin{pmatrix} r_{\alpha_1} e^{i\alpha_1} & r_{\alpha_2} e^{i\alpha_2} & r_{\alpha_3} e^{i\alpha_3} & r_{\alpha_4} e^{i\alpha_4} \end{pmatrix}^T, \quad (4.7)$$

and the states Eve uses as

$$|\psi_1\rangle = \begin{pmatrix} r_{\phi_1} e^{i\phi_1} & r_{\phi_2} e^{i\phi_2} \end{pmatrix}^T, \quad (4.8)$$

$$|\psi_2\rangle = \begin{pmatrix} r_{\omega_1} e^{i\omega_1} & r_{\omega_2} e^{i\omega_2} \end{pmatrix}^T. \quad (4.9)$$

Normalization of the state vectors implies

$$r_{\alpha_1}^2 + r_{\alpha_2}^2 + r_{\alpha_3}^2 + r_{\alpha_4}^2 = 1, \quad (4.10)$$

$$r_{\phi_1}^2 + r_{\phi_2}^2 = 1, \quad (4.11)$$

$$r_{\omega_1}^2 + r_{\omega_2}^2 = 1. \quad (4.12)$$

The moduli  $r_{\alpha_j}$  are conveniently parametrized by three angles  $\bar{\theta} = (\theta_1, \theta_2, \theta_3)$  as the surface of a four-dimensional sphere:

$$\begin{cases} r_{\alpha_1} = \cos \theta_1 \\ r_{\alpha_2} = \sin \theta_1 \cos \theta_2 \\ r_{\alpha_3} = \sin \theta_1 \sin \theta_2 \cos \theta_3 \\ r_{\alpha_4} = \sin \theta_1 \sin \theta_2 \sin \theta_3. \end{cases} \quad (4.13)$$

The moduli of Eve's qubits represent two circles for which two angles  $\Phi$  and  $\Omega$  suffice as

$$r_{\phi_1} = \cos \Phi \quad \text{and} \quad r_{\phi_2} = \sin \Phi, \quad (4.14)$$

$$r_{\omega_1} = \cos \Omega \quad \text{and} \quad r_{\omega_2} = \sin \Omega. \quad (4.15)$$

After several simplifying steps, one obtains

$$E_{\text{mm}} = \left\{ 2 \left[ 1 - \min_{\bar{\theta}, \bar{\alpha}} \max_{\Phi, \Omega, \bar{\phi}, \bar{\omega}} G(\bar{\theta}, \bar{\alpha}, \Phi, \Omega, \bar{\phi}, \bar{\omega}) \right] \right\}^{1/2}, \quad (4.16)$$

where the complex argument parameters are gathered into vectors

$$\bar{\alpha} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4); \quad \bar{\phi} = (\phi_1, \phi_2); \quad \bar{\omega} = (\omega_1, \omega_2). \quad (4.17)$$

The function  $G$ , which Eve tries to maximize and whose maximum Alice and Bob attempt to minimize, is

$$\begin{aligned} G(\bar{\theta}, \bar{\alpha}, \Phi, \Omega, \bar{\phi}, \bar{\omega}) := & \cos \Phi [\cos \Omega \cos(\alpha_1 - \phi_1 - \omega_1) \cos \theta_1 \\ & + \sin \Omega \cos(\alpha_2 - \phi_1 - \omega_2) \sin \theta_1 \cos \theta_2] \\ & + \sin \Phi [\cos \Omega \cos(\alpha_3 - \phi_2 - \omega_1) \sin \theta_1 \sin \theta_2 \cos \theta_3 \\ & + \sin \Omega \cos(\alpha_4 - \phi_2 - \omega_2) \sin \theta_1 \sin \theta_2 \sin \theta_3] . \end{aligned} \quad (4.18)$$

Global bounds for the error follow from the extreme values of  $G$

$$-1 \leq G \leq 1 \quad \Rightarrow \quad 0 \leq E_{\text{mm}} \leq 2 . \quad (4.19)$$

Because Alice and Bob wish to maximize the norm in Eq. (4.6), it is of no use to consider parameters in the set  $\{\bar{\theta}, \bar{\alpha}\}$  that have no effect on the minimal value Eve is trying to achieve. We show that it is in fact sufficient to consider the maximization with three of the phases  $\alpha_j$  fixed—varying them cannot increase the minimum. Firstly, the global phase of the pair  $|\psi\rangle$  offers Alice and Bob no advantage, as it is directly reproduced by Eve. Secondly, Eve can apply any single-qubit gates to  $|\psi_1\rangle$  and  $|\psi_2\rangle$ . For instance, Eve can freely choose  $\beta_1, \beta_2, \beta_3 \in \mathbb{R}$  and apply the gate

$$e^{i\beta_0} (e^{i\beta_1\sigma_z} \otimes e^{i\beta_2\sigma_z}) = \begin{pmatrix} e^{i(\beta_0+\beta_1+\beta_2)} & 0 & 0 & 0 \\ 0 & e^{i(\beta_0+\beta_1-\beta_2)} & 0 & 0 \\ 0 & 0 & e^{i(\beta_0-\beta_1+\beta_2)} & 0 \\ 0 & 0 & 0 & e^{i(\beta_0-\beta_1-\beta_2)} \end{pmatrix} \quad (4.20)$$

to her qubit pair. The global phase shift is implemented by  $\beta_0$ . By choosing the  $\beta_j$  as

$$\begin{cases} \beta_0 + \beta_1 + \beta_2 = \alpha_1 \\ \beta_0 + \beta_1 - \beta_2 = \alpha_2 \\ \beta_0 - \beta_1 + \beta_2 = \alpha_3 \end{cases} \Leftrightarrow \begin{cases} \beta_0 = \frac{1}{2}(\alpha_2 + \alpha_3) \\ \beta_1 = \frac{1}{2}(\alpha_1 - \alpha_3) \\ \beta_2 = \frac{1}{2}(\alpha_1 - \alpha_2) \end{cases} , \quad (4.21)$$

Eve can reproduce the phases  $\alpha_1, \alpha_2, \alpha_3$  in  $|\psi\rangle$ . Therefore, Alice and Bob may as well fix their value. Similar reasoning can be applied to the amplitudes  $r_\Delta$ , which is, however, not carried out here.

### 4.2.2 Solution

Having fixed  $\alpha_1 = \alpha_2 = \alpha_3 = 0$ , we solve for  $E_{\text{mm}}$ , optimizing over  $\bar{\theta}, \alpha_4$  and  $\Phi, \Omega, \bar{\phi}, \bar{\omega}$ . We use the built-in numerical optimization function of *Mathematica*



version 5.1.0.0 by Wolfram Research, Inc. As with any numerical maximization or minimization method, there are no guarantees that the found optimum is the global optimum. As discussed below, however, it is likely that a global optimum is found.

For the maximization of  $G$  over Eve's parameters, we employ the *RandomSearch* optimization method which generates, in this case, 100 random parameter starting points for the standard *FindMinimum* function. *RandomSearch* is a suitable method for maximizing  $G$ , since  $G$  is a continuous and smooth function in all its arguments [81]. The minimization of this maximum is performed with the *SimulatedAnnealing* method. Simulated annealing is a well-known optimization method that has similarities to the process of a physical system cooling down. First, the method randomly generates a set of starting points for the parameters. It also generates a random direction in the parameter space for each point. If moving to the selected direction satisfies the optimization goal better, the move is accepted, whereas if the move satisfies the goal worse, it is accepted with probability  $p_m$ . The probability  $p_m$  decreases with each iteration, and also depends on how well the move satisfies the optimization goal. This procedure is repeated until the method stays at the same point for sufficiently many iterations, or until a predefined number of iterations is exceeded. Simulated annealing is a universally valid optimization method.

### 4.2.3 Results

We find that  $E_{\text{mm}} = 0.673$ . This is achieved by choosing  $\bar{\theta} = (1.228, 0.848, -0.499)$  and  $\alpha_4 = 0.474$  with  $\bar{\alpha} = (0, 0, 0, \alpha_4)$ . To further confirm the result, the maximization of  $G$  over Eve's parameters was also performed with the differential evolution, Nelder-Mead, and simulated annealing methods, in addition to *RandomSearch*. The details of the methods are not discussed here, for more information, see, e.g., Ref. [81]. Many different initial values were also tested. All these methods and all tested initial values resulted in the same maximum for  $G$ . Therefore, we are confident that we indeed have obtained the global maximum of  $G$  for the values of  $\bar{\theta}$  and  $\bar{\alpha}$  given above. The optimal choice of Eve's parameters is not unique. Due to finite computing resources, no such intensive testing was applied to the more demanding minimization of the maximum of  $G$  over  $\bar{\theta}$  and  $\bar{\alpha}$ . Hence, we only state that the

obtained values for  $\bar{\theta}$  and  $\bar{\alpha}$  are the optimal choice for Alice and Bob with high probability. That is, we settle for the confidence the simulated annealing method provides.

The obtained optimal values for  $\bar{\theta}$  and  $\bar{\alpha}$  approximately correspond to the state

$$|\psi\rangle = \begin{pmatrix} 0.34 & 0.62 & 0.62 & -0.30 - 0.15i \end{pmatrix}^T. \quad (4.22)$$

The best Eve can do to approximate  $|\psi\rangle$  with her two unentangled qubits is to choose, for example,  $\Phi = 2.365$ ,  $\Omega = 0.797$ ,  $\phi_1 = 1.243$ ,  $\phi_2 = 3.034$ ,  $\omega_1 = 2.801$ , and  $\omega_2 = 1.472$ . This approximately corresponds to the state

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} 0.31 + 0.39i & 0.46 - 0.21i & 0.44 - 0.21i & -0.10 - 0.49i \end{pmatrix}^T. \quad (4.23)$$

To recapitulate, if Alice and Bob provide Eve with the state in Eq. (4.22), it is guaranteed that the error in Eve's approximation is at least 0.673.

## 4.3 Analysis of an intercept-resend attack

In this section, we aim at answering the question: “Assuming Eve uses the intercept-resend attack strategy, which  $U$  should Alice and Bob choose?” In the BB84 protocol, the IR attack strategy is less efficient than an optimal incoherent attack. However, it is not clear that the same holds for our augmented protocol. Moreover, if a transformation  $U$  provides Alice and Bob advantage against an IR attack, it is likely that the advantage stands, at least to some extent, against more sophisticated attacks, as well.

### 4.3.1 Parametrization of $U$

An arbitrary two-qubit gate has 16 degrees of freedom. For Alice and Bob's purposes however, several of these are useless. Firstly, one degree of freedom arises from the global phase shift introduced by the gate. It is well known that the global phase of the qubit pair is irrelevant. We can always choose the global phase such that the determinant of the gate is +1. Thus we can restrict our search to the special unitary group  $SU(4)$ , the members of which have  $4^2 - 1 = 15$  degrees of freedom.

Following the treatment of J. Zhang *et al.* [82], we partition the group  $SU(4)$  into two: the subset of local gates,  $L_4 := SU(2) \otimes SU(2)$ , and the subset of non-local gates,  $NL_4 := SU(4) \setminus SU(2) \otimes SU(2)$ . It is shown in Ref. [82] that any  $U \in SU(4)$  can be decomposed as

$$\begin{aligned} U &= k_2 A(c_1, c_2, c_3) k_1 \\ &= (k_{2,1} \otimes k_{2,2}) \exp \left[ \frac{i}{2} (c_1 \sigma_x \otimes \sigma_x + c_2 \sigma_y \otimes \sigma_y + c_3 \sigma_z \otimes \sigma_z) \right] (k_{1,1} \otimes k_{1,2}), \end{aligned} \quad (4.24)$$

where  $k_i \in L_4$  and thus  $k_{i,j} \in SU(2)$  and the parameters  $c_l \in [0, \pi]$ ,  $l = 1, 2, 3$ .

Quantum circuits are a graphical way of representing quantum information processing, such as the application of a gate  $k_2 A(c_1, c_2, c_3) k_1$  on two qubits. In a quantum circuit diagram, a single horizontal line represents a qubit. A double horizontal line represents a cbit. Time progresses from left to right, and an operation  $O$  targeted to one or more qubits is shown as a box placed on top of the qubits involved in the operation  $O$ .

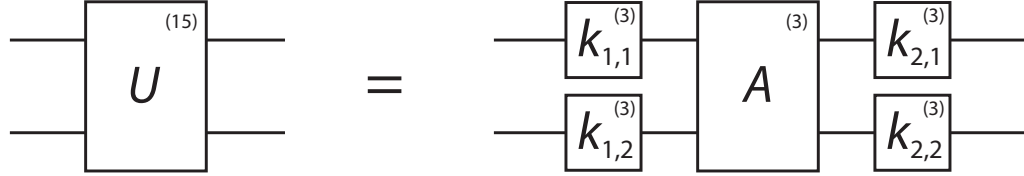


Figure 4.1: Any  $U \in SU(4)$ , shown left, is equal to a decomposition shown on the right. The number of degrees of freedom is shown in parentheses for each gate.

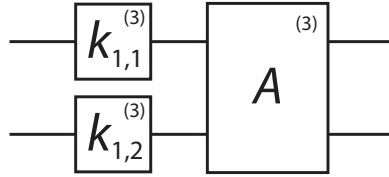


Figure 4.2: A simplified gate model that is at least as useful for Alice and Bob as any other two-qubit transformation. The number of degrees of freedom is displayed in parentheses for each gate.

Figure 4.1 shows on the right the quantum circuit of the decomposed gate  $U$ . The qubits  $|a_1\rangle, |a_2\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$  generated by Alice enter the circuit from the left and depart at the right end after the application of  $U$ . Since we are interested in the security of this protocol, we assume that after the gate  $U$  both qubits travel to Eve. Note that we do not assume that Eve necessarily does anything to either qubit. If Alice employs  $k_2 = k_{2,1} \otimes k_{2,2}$ , Eve can always undo and redo it perfectly with the single-qubit gates  $k_{2,1}^\dagger, k_{2,2}^\dagger$  and  $k_{2,1}, k_{2,2}$ . Hence,  $k_2$  is useless to Alice and Bob, and we may further restrict our search for a good gate  $U$  to gates of the form  $A(c_1, c_2, c_3)k_1$ , shown in Fig. 4.2. Thus we are left with 9 degrees of freedom for  $U$ .

### 4.3.2 Explicit matrices

To be able to simulate the amended protocol, we have to write down the matrix for the transformation  $U$  explicitly. Any single-qubit gate  $k \in \text{SU}(2)$  can be written as

$$k(a_1, a_2, a_3) = \begin{pmatrix} e^{ia_1} \cos a_2 & e^{ia_3} \sin a_2 \\ -e^{-ia_3} \sin a_2 & e^{-ia_1} \cos a_2 \end{pmatrix}. \quad (4.25)$$

The explicit matrix for the non-local gate  $A(c_1, c_2, c_3) = \exp[i(c_1 \sigma_x \otimes \sigma_x + c_2 \sigma_y \otimes \sigma_y + c_3 \sigma_z \otimes \sigma_z)/2]$  is obtained by first finding the eigensystem of the hermitian operator  $B := c_1 \sigma_x \otimes \sigma_x + c_2 \sigma_y \otimes \sigma_y + c_3 \sigma_z \otimes \sigma_z$  and then applying

$$f(B) = \sum_j f(\lambda_j) |\lambda_j\rangle \langle \lambda_j|, \quad (4.26)$$

where  $\lambda_j$  are the eigenvalues and  $|\lambda_j\rangle$  the corresponding eigenvectors of the hermitian operator  $B$ . Equation (4.26) is a direct consequence of the spectral decomposition theorem and holds for any analytic function  $f$ . In this case,  $f(\cdot) = e^{i(\cdot)/2}$ . The result is

$$A(c_1, c_2, c_3) = \begin{pmatrix} e^{ic_3/2} \cos\left(\frac{c_1-c_2}{2}\right) & 0 & 0 & ie^{ic_3/2} \sin\left(\frac{c_1-c_2}{2}\right) \\ 0 & e^{-ic_3/2} \cos\left(\frac{c_1+c_2}{2}\right) & ie^{-ic_3/2} \sin\left(\frac{c_1+c_2}{2}\right) & 0 \\ 0 & ie^{-ic_3/2} \sin\left(\frac{c_1+c_2}{2}\right) & e^{-ic_3/2} \cos\left(\frac{c_1+c_2}{2}\right) & 0 \\ ie^{ic_3/2} \sin\left(\frac{c_1-c_2}{2}\right) & 0 & 0 & e^{ic_3/2} \cos\left(\frac{c_1-c_2}{2}\right) \end{pmatrix}. \quad (4.27)$$

### 4.3.3 Simulation

We simulate the progress of our protocol with different transformations  $U$  and observe the QBER induced by Eve and Eve's mutual information on Alice's sifted key. Eve is assumed to employ the intercept-resend attack. She is allowed to choose between a projective measurement in either the  $z$  or  $x$  basis and not to perform any measurement individually for each of the two transmitted qubits. In the original BB84 protocol, it is clear that the  $z$  and  $x$  bases are the best measurement bases for Eve. In our augmented protocol, this is not necessarily true. For simplicity, however, we restrict Eve's measurements to these bases.

#### Preliminary remarks

Let  $A$  denote the random variable that fully determines which pair of BB84 states  $|a_1\rangle|a_2\rangle$  Alice constructs prior to the application of the non-local gate. That is,  $A$  takes its values with uniform probability from the set  $\{00, 01, 10, 11, 0+, 0-, 1+, 1-, +0, +1, -0, -1, ++, +-, -+, --\}$ . The physical state is obtained for each outcome  $a_1a_2$  by surrounding the label with the bracket construct  $|a_1a_2\rangle$ . Let us re-label the outcomes with integers in the range  $[0, 15]$ , in the order they are presented above, with the symbol  $a$ . For example,  $a_1 = +$  and  $a_2 = 1$  is expressed as  $a = 9$ .

Let  $E$  denote the random variable that gives the joint result of Eve's measurements, and let  $e$  denote the outcome of  $E$ . The value of  $e \in \{0, 1, 2, 3\}$  is obtained by interpreting the separate results  $e_1, e_2 \in \{0, 1\}$  as a binary number  $e_1e_2$  with  $e_2$  as the least significant bit.

We may calculate Eve's mutual information on Alice's sifted key as her mutual information  $I(A, E)$  on the random variable  $A$ . These two mutual informations are equal, which can be shown in exactly the same way as was done in Sec. 3.1.5 for one cbit and qubit in the original BB84 protocol. Due to the close similarities, the proof is not reproduced for the case of two cbits and qubits.

Because of finite computing resources, we use only the non-local gate  $A(c_1, c_2, c_3)$  in our simulation. It is likely that using in addition the local gate  $k_1$  benefits Alice and Bob, but it is also plausible that part of this gate commutes with the gate  $A$  in

the sense that Eve would be able to undo  $k_1$  partially with single-qubit gates. This possibility is not investigated further in this Thesis.

Figure 4.3 shows the quantum transmission phase of the protocol and the attack we simulate as a quantum circuit for one qubit pair. In practice, Eve's measurement scheme may be such that the measured qubits are demolished. In this case, she creates new physical qubits in the logical state corresponding to her measurement result. This is equivalent to performing a non-demolishing projective measurement.

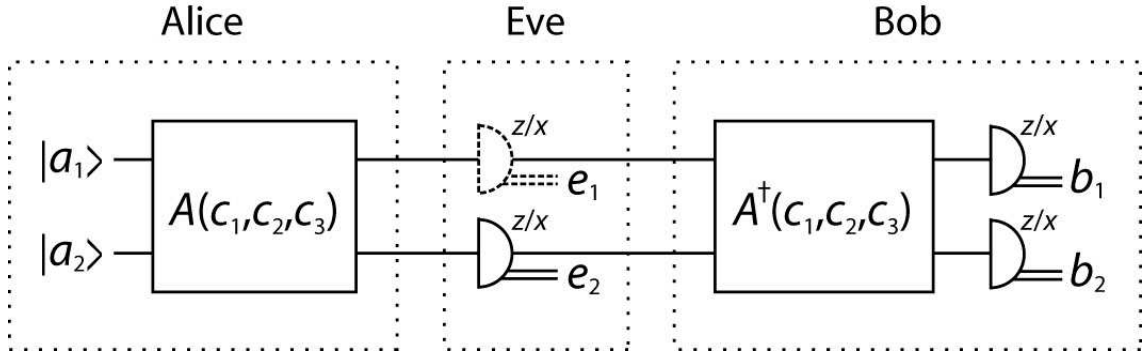


Figure 4.3: The full quantum circuit of the proposed protocol and the attack for a qubit pair. The interleaving classical communication between Alice and Bob is not shown. The circuit is run a large number of times in each use of the protocol. The actions of each participant are enclosed in dotted boxes. A semicircle represents a projective measurement. Eve performs measurements but not necessarily on the first qubit. Symbols  $e_1$  and  $e_2$  denote Eve's measurement results, and  $b_1$  and  $b_2$  Bob's results which are assumed to contribute to the sifted key.

The protocol is sampled over a large number of different gates  $A(c_1, c_2, c_3)$ . We run a numerical *Mathematica* code that records  $I(A, E)$  and the QBER observed by Bob for Eve's allowed measurement bases and a given gate  $A$ . The algorithm is presented below. The code is run with different values of the parameters  $c_1, c_2, c_3$  for the gate  $A$ . Each  $c_i$  takes values in the interval  $[0, \pi]$  with  $\frac{\pi}{32}$  steps. That is, we sample the three-dimensional parameter space uniformly with  $33^3 \approx 36000$  points. This is not an exhaustive survey of the possibilities of the use of a non-local gate, but as long as Eve obeys the presented assumptions, the obtained maximum of  $I(A, E)$  holds for the given parameters  $c_1, c_2, c_3$ .

The following paragraphs describe phase-by-phase the algorithm used in the simulation of our protocol. The algorithm has not been optimized for performance, but instead kept in a form close to the underlying mathematics and physics. In the actual code, all calculation is done numerically. Every transmission state of the original BB84 protocol is assumed to occur with equal probability, and we only consider transmissions that contribute to the sifted key.

### Phase 1: Non-local transformation

First, the gate  $A(c_1, c_2, c_3)$  is applied to all 16 possible qubit-pair states used in the original BB84 protocol.

$$|\psi_{a_1 a_2}\rangle = A(c_1, c_2, c_3)|a_1\rangle|a_2\rangle, \quad a_1, a_2 \in \{0, 1, +, -\}. \quad (4.28)$$

The qubit in the left slot, i.e., originally in state  $|a_1\rangle$ , is sent first.

### Phase 2: Eve's first measurement

Eve may choose not to measure either of the two qubits. Since we apply a symmetric gate to the qubit pair, measuring only the first qubit is equivalent to measuring only the second qubit. Therefore, it suffices to simulate the protocol with Eve skipping the measurement only on the first qubit. If Eve does not measure either qubit, there is nothing to simulate.

If Eve has chosen to measure the first qubit, the measurement is calculated in the  $z$  and  $x$  bases. Based on Eq. (2.22), the probability of measurement outcome  $e_1$  is

$$p(E_1 = e_1 | P_{E1} = \varepsilon_1, A = a) = \langle \psi_{a_1 a_2} | (P_{e_1}^{\varepsilon_1} \otimes I) | \psi_{a_1 a_2} \rangle, \quad (4.29)$$

where  $E_n$  is the random variable corresponding to the result of Eve's measurement of qubit  $n \in \{1, 2\}$  and  $\varepsilon_1$  is Eve's basis choice. The post-measurement state is

$$|\psi_{a_1 a_2}(e_1, \varepsilon_1)\rangle := (P_{e_1}^{\varepsilon_1} \otimes I) |\psi_{a_1 a_2}\rangle / \sqrt{p(e_1 | \varepsilon_1, a)}, \quad (4.30)$$

in accordance with Eq. (2.23). However, if  $p(e_1 | \varepsilon_1, a) = 0$ , we define

$$|\psi_{a_1 a_2}(e_1, \varepsilon_1)\rangle := \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}^T. \quad (4.31)$$

If Eve does not measure the first qubit, we define  $|\psi_{a_1 a_2}(e_1, \varepsilon_1)\rangle := |\psi_{a_1 a_2}\rangle$  and mark the probabilities of all outcomes as 1, which is mathematically inconsistent, but is later taken into account.

### Phase 3: Eve's second measurement

Eve chooses a measurement basis for the second qubit and applies a projective measurement in the  $z$  or  $x$  basis. The probability of measurement outcome  $e_2$  is

$$\begin{aligned} p(E_2 = e_2 | E_1 = e_1, P_{E1} = \varepsilon_1, P_{E2} = \varepsilon_2, A = a) \\ = \langle \psi_{a_1 a_2}(e_1, \varepsilon_1) | (I \otimes P_{e_2}^{\varepsilon_2}) | \psi_{a_1 a_2}(e_1, \varepsilon_1) \rangle, \end{aligned} \quad (4.32)$$

where  $\varepsilon_2$  is Eve's basis choice for the second measurement. If the result  $e_1$  is impossible, the probability in Eq. (4.32) is correctly zero, since in this case the state vector is the zero vector. After both of Eve's measurements, Bob is in possession of the qubit pair which is in state

$$|\psi_{a_1 a_2}(e_1, \varepsilon_1, e_2, \varepsilon_2)\rangle := (I \otimes P_{e_2}^{\varepsilon_2}) |\psi_{a_1 a_2}(e_1, \varepsilon_1)\rangle / \sqrt{p(e_2 | e_1, \varepsilon_1, \varepsilon_2, a)}. \quad (4.33)$$

Again, if  $p(e_2 | e_1, \varepsilon_1, \varepsilon_2, a) = 0$ , we define the state to be the zero vector.

### Mutual information

We allow Eve to choose the measurement basis independently for each qubit and calculate  $I(A, E)$  for the different basis choices. Since the QBER also depends on the measurement basis, we must keep track of the results of all the choices to obtain a complete picture of Eve's capabilities. Because we consider the different basis choices separately, we may omit the explicit conditioning on the basis in all probabilities.

To be able to compare our results with other QKD protocols, we calculate Eve's information per bit. The mutual information of  $A$  and  $E$  given by Eq. (2.11) yields Eve's information on a two-bit entity. Thus the mutual information per bit is half of this, i.e.,

$$I(A, E) = \frac{1}{2} [H(A) + H(E) - H(A, E)]. \quad (4.34)$$



The entropy  $H(A)$  is always

$$H(A) = - \sum_{j=0}^{15} p(a) \log p(a) = - \sum_{j=0}^{15} \frac{1}{16} \log \left( \frac{1}{16} \right) = 4 . \quad (4.35)$$

According to Eq. (2.6),

$$\begin{aligned} p(e|a) &= p(E = e_1 e_2 | A = a) \\ &= p(e_2 | e_1, \varepsilon_1, \varepsilon_2, a) p(e_1 | \varepsilon_1, \varepsilon_2, a) , \end{aligned} \quad (4.36)$$

the two factors of which have been calculated in Eqs. (4.29) and (4.32). The entropy of Eve's variable is

$$\begin{aligned} H_m(E) &= - \sum_{e=0}^m p(e) \log p(e) \\ &\stackrel{(2.4)}{=} - \sum_{e=0}^m \left[ \sum_{a=0}^{15} p(e|a) p(a) \right] \log \left[ \sum_{a=0}^{15} p(e|a) p(a) \right] \\ &= - \frac{1}{16} \sum_{e=0}^m \left[ \sum_{a=0}^{15} p(e|a) \right] \left\{ \log \left[ \sum_{a=0}^{15} p(e|a) \right] - 4 \right\} , \end{aligned} \quad (4.37)$$

where  $m = 1$ , if Eve measures only the second qubit, and  $m = 3$ , if Eve measures both qubits. This is justified by noting that if the first measurement is not performed, all probabilities of  $e_1$  are designated value 1 and  $E_2$  does not depend on  $E_1$ , and thus  $p(e|a) = p(e_2|a)$  given by Eq. (4.32).

The joint entropy of  $A$  and  $E$  is

$$\begin{aligned} H_m(A, E) &\stackrel{(2.10)}{=} - \sum_{e=0}^m \sum_{a=0}^{15} p(e, a) \log p(e, a) \\ &\stackrel{(2.2)}{=} - \sum_{e=0}^m \sum_{a=0}^{15} p(e|a) p(a) \log [p(e|a) p(a)] \\ &= - \frac{1}{16} \sum_{e=0}^m \sum_{a=0}^{15} p(e|a) [\log p(e|a) - 4] \\ &= \frac{1}{4} \sum_{e=0}^m \sum_{a=0}^{15} p(e|a) - \frac{1}{16} \sum_{e=0}^m \sum_{a=0}^{15} p(e|a) \log p(e|a) . \end{aligned} \quad (4.38)$$

If  $p(e|a) = 0$  for some  $e$  and  $a$ , we assign value zero to the term  $p(e|a) \log p(e|a)$ .

#### Phase 4: Inverse non-local transformation

Once Bob has received both qubits, he applies  $A^\dagger(c_1, c_2, c_3)$  to the pair, and obtains the state

$$|\psi_{a_1 a_2}^{\text{Bob}}(e_1, \varepsilon_1, e_2, \varepsilon_2)\rangle := A^\dagger(c_1, c_2, c_3)|\psi_{a_1 a_2}(e_1, \varepsilon_1, e_2, \varepsilon_2)\rangle . \quad (4.39)$$

If Eve had not interfered with either qubit, it would be safe to write this as a product state.

#### Phase 5: Bob's first measurement

Bob projectively measures both qubits in correct bases. For the first qubit, the probability of result  $b_1 \in \{0, 1\}$  given  $A = a_1 a_2$  and  $E = e_1 e_2$  is

$$p(b_1|a_1 a_2, e_1 e_2) = \langle \psi_{a_1 a_2}^{\text{Bob}}(e_1, \varepsilon_1, e_2, \varepsilon_2) | \left( P_{b_1}^{\delta_{1,a}} \otimes I \right) | \psi_{a_1 a_2}^{\text{Bob}}(e_1, \varepsilon_1, e_2, \varepsilon_2) \rangle , \quad (4.40)$$

where

$$\delta_{1,a} = \begin{cases} z & \text{if } a \in [0, 7] \\ x & \text{if } a \in [8, 15] \end{cases} . \quad (4.41)$$

If the result  $e_1 e_2$  is impossible, the probability is zero because the state vector is the zero vector. The probability of  $b_1$  given only  $A = a_1 a_2$  is

$$p(b_1|a) \stackrel{(2.5)}{=} \sum_{e=0}^m p(b_1, e|a) \stackrel{(2.6)}{=} \sum_{e=0}^m p(b_1|a, e) p(e|a) . \quad (4.42)$$

Bob's first measurement projects the qubit pair into state

$$|\psi_{a_1 a_2}^{\text{Bob}}(e_1, \varepsilon_1, e_2, \varepsilon_2, b_1)\rangle = P_{b_1}^{\delta_{1,a}} |\psi_{a_1 a_2}^{\text{Bob}}(e_1, \varepsilon_1, e_2, \varepsilon_2)\rangle / \sqrt{p(b_1|a_1 a_2, e_1 e_2)} , \quad (4.43)$$

unless  $p(b_1|a_1 a_2, e_1 e_2) = 0$ , in which case the state is the zero vector.

#### QBER of the first qubit

If the transmission has no errors, the first measurement yields value 0 for  $a \in \mathcal{A}_{10} = \{0, 1, 4, 5, 8, 9, 12, 13\}$ , and value 1 for  $a \in \mathcal{A}_{11} = \{2, 3, 6, 7, 10, 11, 14, 15\}$ . Thus the QBER of the first qubit is, according to Eq. (3.22),

$$\text{QBER}_1 = \frac{1}{16} \left[ \sum_{a \in \mathcal{A}_{10}} p(B_1 = 1|a) + \sum_{a \in \mathcal{A}_{11}} p(B_1 = 0|a) \right] , \quad (4.44)$$

where  $B_i$  is the random variable that yields the result of Bob's  $i$ th measurement.

### Phase 6: Bob's second measurement

Bob measures the second qubit. The probability of getting result  $b_2 \in \{0, 1\}$  given  $A = a_1 a_2$  is

$$\begin{aligned}
 p(b_2|a) &\stackrel{(2.5)}{=} \sum_{b_1=0}^1 p(b_2, b_1|a) \\
 &\stackrel{(2.6)}{=} \sum_{b_1=0}^1 p(b_2|b_1, a) p(b_1|a) \\
 &\stackrel{(2.5)}{=} \sum_{b_1=0}^1 \sum_{e=0}^m p(b_2, e|b_1, a) p(b_1|a) \\
 &\stackrel{(2.6)}{=} \sum_{b_1=0}^1 \sum_{e=0}^m p(b_2|b_1, e, a) p(e|b_1, a) p(b_1|a) \\
 &\stackrel{(2.7)}{=} \sum_{b_1=0}^1 \sum_{e=0}^m p(b_2|b_1, e, a) p(b_1|e, a) \frac{p(e|a)}{p(b_1|a)} p(b_1|a) \\
 &= \sum_{b_1=0}^1 \sum_{e=0}^m p(b_2|b_1, e, a) p(b_1|e, a) p(e|a) . \tag{4.45}
 \end{aligned}$$

The first factor in the term is obtained by calculating

$$p(b_2|b_1, e, a) = \langle \psi_{a_1 a_2}^{\text{Bob}}(e_1, \varepsilon_1, e_2, \varepsilon_2, b_1) | \left( I \otimes P_{b_2}^{\delta_{2,a}} \right) | \psi_{a_1 a_2}^{\text{Bob}}(e_1, \varepsilon_1, e_2, \varepsilon_2, b_1) \rangle , \tag{4.46}$$

where

$$\delta_{2,a} = \begin{cases} z & \text{if } a \in [0, 3] \text{ or } a \in [8, 11] \\ x & \text{if } a \in [4, 7] \text{ or } a \in [12, 15] . \end{cases} \tag{4.47}$$

Again, if result  $b_1$  or result  $e_1 e_2$  is impossible, the probability is zero because the state is the zero vector.

### Total QBER

After an error-free transmission, the second measurement yields value 0 for even values of  $a$  and 1 for odd values of  $a$ . Therefore, the QBER of the second qubit is

$$\text{QBER}_2 = \frac{1}{16} \left[ \sum_{a \text{ even}} p(B_2 = 1|a) + \sum_{a \text{ odd}} p(B_2 = 0|a) \right] . \tag{4.48}$$

The total QBER is the average over the individual error rates:

$$\text{QBER} = \frac{1}{2} (\text{QBER}_1 + \text{QBER}_2) . \quad (4.49)$$

#### 4.3.4 Results

We are interested in finding the maximum of Eve's mutual information on Alice's sifted key,  $I(A, E)$ , for a given QBER observed by Alice and Bob. In the analyzed attack, Eve has six different measurement configurations for each gate  $A(c_1, c_2, c_3)$ . She can measure both qubits in bases  $zz$ ,  $zx$ ,  $xz$ , or  $xx$ , or she can measure only the second qubit, in  $z$  or  $x$  basis. Due to the symmetry of the protocol with respect to the two transmitted qubits, the case where Eve measures only the first qubit needs no analysis—it is equivalent to measuring only the second one. Furthermore, using any of the six configurations, Eve can choose to interfere with only a fraction  $0 \leq \xi \leq 1$  of the transmitted qubit pairs.

Figure 4.4 shows  $I(A, E)$  as a function of QBER for the sampled parameter values in the different measurement configurations. The results are identical for bases  $zx$  and  $xz$ , and very similar for bases  $zz$  and  $xx$ , if Eve measures both qubits. If Eve measures only the second qubit, the results are very similar for both basis choices. The fraction  $\xi = 1$  in all plots.

Which measurement configuration yields most information on Alice's key? For example, consider the situation for the gate  $A\left(\frac{6\pi}{32}, \frac{25\pi}{32}, \frac{5\pi}{32}\right)$ , shown in Fig. 4.5. The filled circle represents Eve measuring only the second qubit. This configuration provides least information and induces least errors. For the same QBER  $\approx 0.24$ , Eve obtains more information with any other configuration by adjusting  $\xi$  properly, illustrated by the dashed and solid lines parametrized by  $0 \leq \xi \leq 1$ . Hence, measuring only one of the qubits does not provide maximal information. In fact, the same reasoning applies for any gate setting  $c_1, c_2, c_3$ , and we therefore ignore this measurement configuration in the following analysis.

By measuring both qubits in the  $z$  basis, denoted by the square in Fig. 4.5, Eve maximizes her information as well as the QBER for the considered gate. Although measuring both qubits in the  $x$  basis, denoted by the triangle, yields less information,

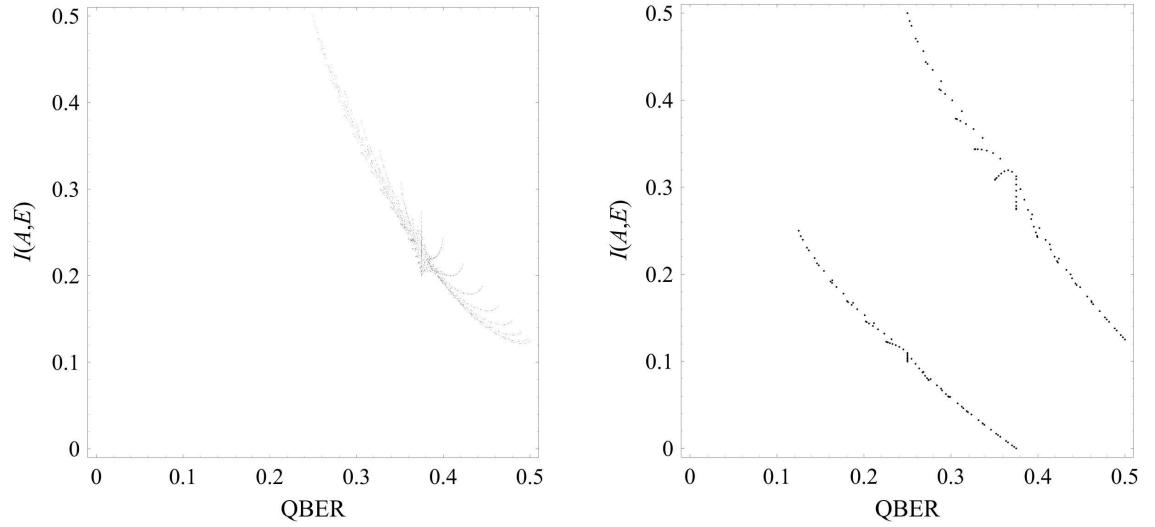


Figure 4.4: Eve's mutual information per bit on Alice's sifted key and the corresponding QBER for the sampled values of  $c_1, c_2, c_3$ , and  $\xi = 1$ . The left panel shows the case where Eve measures both qubits and chooses  $zx$  or  $xz$  as her measurement bases. In the right panel, the lower set of points corresponds to Eve measuring only the second qubit in either basis, and the upper set to Eve measuring both qubits in the same basis. The upper envelope curve of the set in the left panel is the lower envelope curve for the upper set in the right panel.

the relative decrease in the QBER is larger. Thus, for any QBER up to that of the triangle, the  $xx$  bases provide most information. That is, the slope of the  $\xi$  line is larger for the  $xx$  bases. Furthermore, as is shown in Fig. 4.4, for  $\xi = 1$ , the induced QBER is always at least 25%. Having observed a QBER this high, Alice and Bob would most likely abort the protocol. Hence, Eve should always adjust  $\xi < 1$  such that the QBER is well below 25%, and choose the configuration providing the largest slope for the line and thus maximal information. For any gate  $A$ , this configuration always involves measuring both qubits in either the  $z$  basis or the  $x$  basis, and hence we choose this to be Eve's configuration. This result is consistent with the symmetry of the gate  $A$ —there is no reason why it would be beneficial to employ different measurement bases for the qubits. Figure 4.6 shows the mutual information as a function of QBER for the selected configuration and  $\xi = 1$ . For each sampled gate, the maximal information is at most 0.011 bits more than that given by the configuration corresponding to the largest slope.

The plot in Fig. 4.6 is generated as follows. For  $(c_1, c_2, c_3) = (0, 0, 0)$  the mutual information is 0.5 and the QBER 25%. This is consistent with the original BB84, since  $A(0, 0, 0)$  is just the two-qubit identity transformation. The smallest information and the highest QBER, point  $(0.5, 0.125)$ , is achieved with, e.g., the gate  $A(0, \frac{\pi}{2}, 0)$ . The lower envelope curve for the set of points in Fig. 4.6 is obtained by sweeping  $c_2 \in [0, \frac{\pi}{2}]$  while keeping  $c_1 = c_3 = 0$ . Each of the concave arcs above the envelope are obtained by sweeping over  $c_3$  for different values of  $c_2$ . For instance, if  $c_1 = 0$  and  $c_2 = \frac{13\pi}{16}$ , increasing  $c_3$  from 0 to  $\frac{\pi}{2}$  produces the dashed arc in Fig. 4.6. For different values of  $c_1$ , the sweeps over  $c_2$  and  $c_3$  yield arcs of different shape in the same set of points. We thus observe that adjusting  $c_1$  is redundant, the same effect is achieved by an appropriate choice of  $c_2$  and  $c_3$ .

Let us compare our protocol with the original BB84. Figure 4.7 shows Eve's maximal information as a function of QBER for BB84 and for three representative gates in our protocol. The oblique lines are obtained by varying  $\xi \in [0, 1]$ . The solid line denotes BB84 and the densely dashed lines our protocol for settings  $c_1 = c_3 = 0$  and  $c_2 = \frac{\pi}{8}, \frac{\pi}{4}, \frac{\pi}{2}$ . Our protocol provides Eve less information and induces more errors in the sifted key for a given  $\xi$ . For instance, by employing gate  $A(0, \frac{\pi}{8}, 0)$ , Eve's information is decreased by 0.0875 bits and the QBER increased by only 0.037,

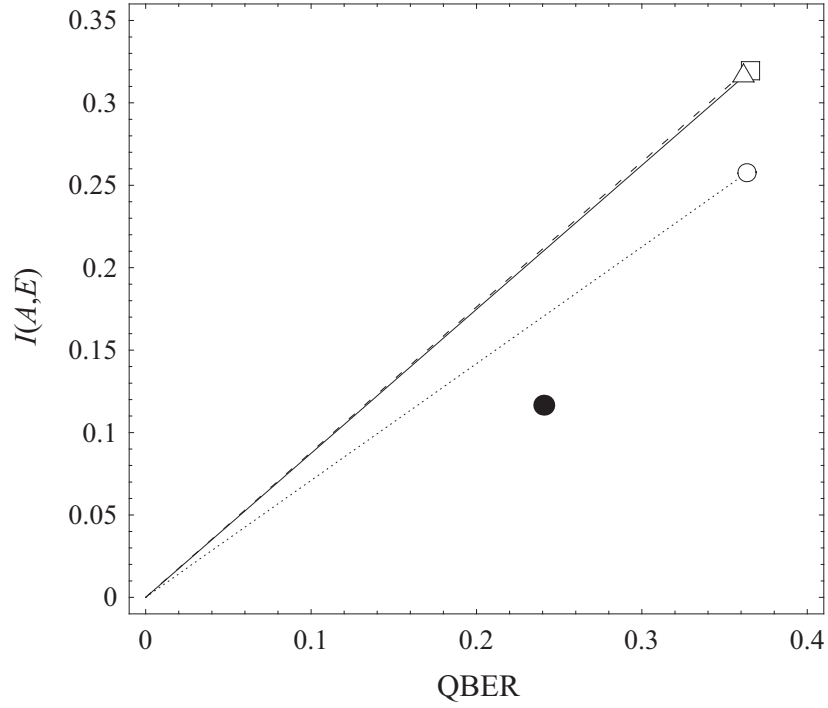


Figure 4.5: Eve's information on Alice's key and the induced QBER for the gate  $A\left(\frac{6\pi}{32}, \frac{25\pi}{32}, \frac{5\pi}{32}\right)$ . The filled circle corresponds to Eve measuring only the second qubit. The open symbols correspond to the cases where Eve measures both qubits: The circle denotes the  $zx$  or  $xz$  bases, the square bases  $zz$ , and the triangle bases  $xx$ . The mutual information and the QBER are slightly larger for the  $zz$  than for the  $xx$  choice. The solid, dashed, and dotted lines show Eve's information for  $\xi \in [0, 1]$  for bases  $zz$ ,  $xx$ , and  $xz$ , respectively.

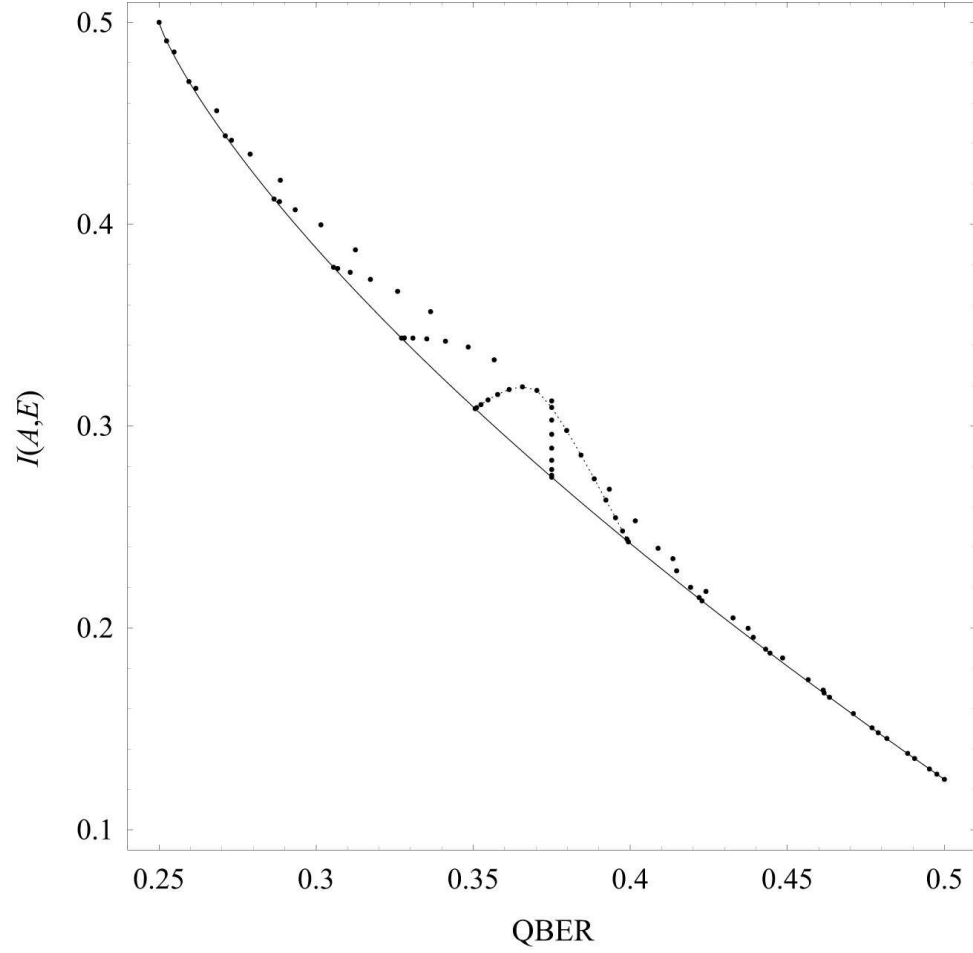


Figure 4.6: Eve's information on Alice's key and the induced QBER for the sampled gates and  $\xi = 1$ , given that Eve chooses the measurement configuration yielding the largest slope for the  $\xi$ -parametrized line. The solid line illustrates the lower envelope of the set, obtained by sweeping over  $c_2$  for  $c_1 = c_3 = 0$ . The dashed line is obtained by sweeping over  $c_3$  for  $c_1 = 0$  and  $c_2 = \frac{13\pi}{16}$ .



for  $\xi = 1$ . In BB84, the incoherent attack provides approximately 0.13 bits more information than the IR attack for a 20% QBER, as is shown in Fig. 3.2. In our protocol, Eve's information for the same QBER can be reduced from 0.4 to 0.05—much more than what is gained by applying an incoherent attack in BB84. The difference is significant for any QBER less than 25%.

The error correction phase provides Eve further information. Equation (2.12) gives a lower bound on the number of bits Alice and Bob need to exchange to correct the errors, with an error probability of  $p = \text{QBER}$  in each bit. The bound is valid for an error process affecting each bit individually, but in our protocol, the errors in the bits obtained from one qubit pair are correlated due to entanglement. However, we can apply the bound to our protocol as well, since correcting pairwise correlated errors cannot be more demanding than correcting independent errors. That is, Alice and Bob can treat the errors as uncorrelated. Because the number of exchanged bits only depends on the QBER, the differences of the lines in Fig. 4.7 remain the same after adding to them the information provided by the error-correction step. Thus, for a given QBER, our protocol provides Eve strictly less information with  $c_2$  and  $c_3$  chosen properly, assuming that Eve uses the described IR attack.

Which gate  $A(c_1, c_2, c_3)$  should Alice and Bob choose? The answer is complicated by the fact that any practical implementation of the protocol includes a quantum channel with a finite error rate. Eve's interference acts as an approximate, although poor, model for the noise in the quantum channel. While the choice  $A(0, \frac{\pi}{2}, 0)$  limits Eve's information most effectively for any QBER, it also presumably amplifies the noise in the quantum channel the most. Whether this amplification is tolerable depends on the noise. However, since Eve's information decreases rapidly compared to the increase in QBER in the upper part of the envelope curve shown in Fig. 4.7, it is plausible that even for a very noisy channel a non-identity gate benefits Alice and Bob. Moreover, the noise of a practical quantum channel decreases as technology advances.

For instance, assume that Alice and Bob employ the gate  $A(0, \frac{\pi}{2}, 0)$  corresponding to the lowest dashed line in Fig. 4.7. Assume also that the inherent noise of the used quantum channel results in a QBER of at most 10%. If Eve's interference is used as a model for the noise, the QBER is doubled by the gate, since  $\text{QBER} =$

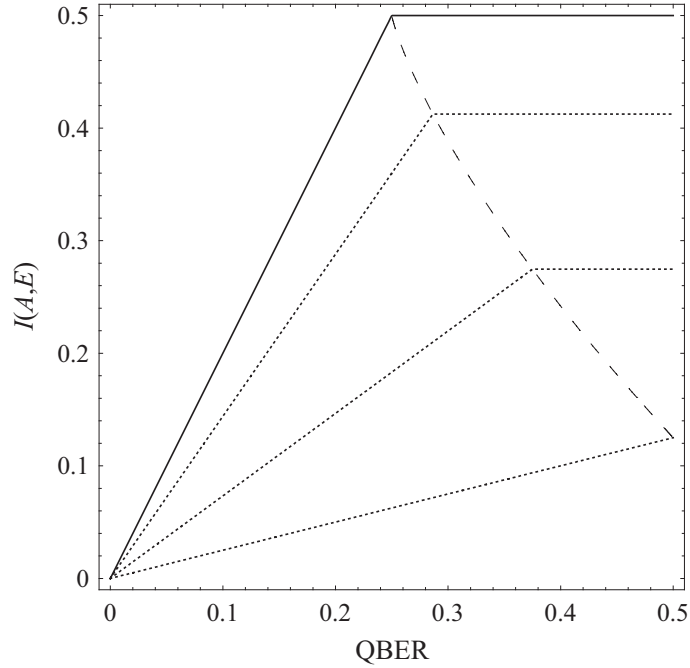


Figure 4.7: Eve's maximal mutual information and the induced QBER for BB84 (solid line) and for our protocol with gate settings  $c_2 = \frac{\pi}{8}, \frac{\pi}{4}, \frac{\pi}{2}$  and  $c_1 = c_3 = 0$ , denoted by the uppermost, middle, and lowest dashed line, respectively. Eve employs an IR attack. The sparsely dashed line denotes the envelope curve of the set shown in Fig. 4.6.

$\xi/4$  without the gate, and  $\text{QBER} = \xi/2$  with the gate. Hence, we assume that if the gate is employed, Alice and Bob must accept a 20% QBER. Without the gate, Eve's maximal information can be limited to 0.2 bits, and with the gate to 0.05 bits. That is, the gate reduces Eve's information to  $1/4$  of that in BB84 even if the noise is taken into account. Exactly which gate to employ depends on the actual noise of the realized quantum channel, however.

## 4.4 EPR-pair attack

Since Alice and Bob utilize entanglement to keep their key a secret, it is an intuitive idea for Eve to also make use of this resource. One way of taking advantage of en-

tanglement in eavesdropping is to send qubits of an EPR pair, defined in Eq. (3.33), to Bob. Let us label the qubits of the EPR pair as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2) . \quad (4.50)$$

After intercepting the first qubit of the transmitted pair, Eve sends qubit 1 of an EPR pair to Bob while keeping qubit 2 for herself. Bob acknowledges the reception of the first qubit, and Alice sends the second qubit which Eve also intercepts. Eve can, e.g., measure the intercepted qubits, and based on the result, apply a single-qubit transformation to the second qubit of the EPR pair which she then sends to Bob. More complicated transformations involving the intercepted qubits are also possible. Eve has thus sent Bob a qubit pair in an entangled state one qubit at a time, and has partial control over the state of the pair after learning the measurement results for both intercepted transmissions.

For instance, assume that Alice and Bob have chosen  $U_1 := \text{CNOT}(H \otimes I)$  as their two-qubit unitary transformation. CNOT is the non-local controlled-not operation which transforms input states as

$$\text{CNOT: } \begin{cases} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{cases}$$

and  $H$  is the Hadamard gate that transforms  $|0\rangle \rightarrow (|0\rangle + |1\rangle)/\sqrt{2}$  and  $|1\rangle \rightarrow (|0\rangle - |1\rangle)/\sqrt{2}$ . The only BB84 states  $|a_1\rangle|a_2\rangle$  not resulting in a tensor product state with the application of  $U_1$  are states  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ . These states are transformed into the Bell states by  $U_1$  as

$$U_1|00\rangle = |\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2} , \quad (4.51)$$

$$U_1|01\rangle = |\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2} , \quad (4.52)$$

$$U_1|10\rangle = |\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2} , \quad (4.53)$$

$$U_1|11\rangle = |\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2} . \quad (4.54)$$

Assume that Eve has some way of knowing if Alice uses the  $z$  basis for the initial state  $|a_1\rangle|a_2\rangle$ . This capability would, of course, severely compromise the security of

any BB84-based QKD protocol. Nevertheless, let us demonstrate how Eve could in this case eavesdrop on the transmission and still preserve its entanglement. If Alice has chosen some other combination of bases than  $zz$  for the qubits, Eve attacks the unentangled transmission using any strategy suitable for the original BB84 protocol. However, if Alice's choice of bases is  $zz$ , Eve knows to expect a transmission of a qubit pair in one of the Bell states, and does the following.

Eve intercepts and stores the first transmitted qubit in short-term quantum memory, and immediately sends qubit 1 of the pair in Eq. (4.50) to Bob. She then intercepts and stores the second transmitted qubit and is thus in possession of the transmitted qubit pair as well as the second qubit of the EPR pair. Eve undoes  $U_1$  by applying  $U_1^\dagger = (H \otimes I)\text{CNOT}$  to the intercepted pair, after which she measures the qubits in  $z$  basis, thus recovering  $a_1$  and  $a_2$  exactly. Based on the result, Eve chooses a single-qubit gate

$$E_{a_1 a_2} = I (\sigma_x)^{a_2} (\sigma_z)^{a_1} , \quad (4.55)$$

which she applies to qubit 2 of the EPR pair. This transforms the pair to the state that Alice transmitted, i.e.,  $(I \otimes E_{a_1 a_2}) |\Phi^+\rangle = U_1 |a_1\rangle |a_2\rangle$ . Eve sends the second qubit to Bob, who applies  $U_1^\dagger$  to the qubit pair. Bob measures the qubits in the  $z$  basis, and recovers  $a_1$  and  $a_2$ . That is, Bob observes a zero QBER while Eve has full knowledge about the key bits Alice and Bob established, given that Alice used the  $zz$  basis. Note that this result only applies if Alice's basis choices are available to Eve at the time of the quantum transmission—a feature that would render the original BB84 protocol useless. The utilization of entanglement in eavesdropping is not discussed further in this Thesis.

# Chapter 5

## Conclusions

We have introduced and studied the properties of a novel BB84-based protocol for quantum key distribution. The proposed protocol utilizes entanglement of the transmitted quantum states to provide advantage against an eavesdropper. We derived a practical model for the entangling transformation, and simulated the protocol numerically over a subset of the transformations. We considered the security of the protocol under an intercept-resend attack. In the simulation, we recorded the information of the eavesdropper on the established key and the quantum bit error rate induced by the attack.

We find that entangling the states of the transmitted qubit pairs properly yields significant advantage to the legitimate users. The maximal mutual information available to an eavesdropper can be controlled in the range from 0.125 to 0.5 bits. Decreasing the maximal information increases the quantum bit error rate to at most 50%. For a given quantum bit error rate below 25%, the maximum information that an intercept-resend attack provides is reduced by a factor of eight. Since eavesdropping causes more disturbance to the quantum transmission than in the original protocol, an eavesdropper is detected more easily. In other words, for a given error rate, an eavesdropper must reduce his or her interference with the quantum channel, and thus acquire less information.

In practice, the entangling transformation also amplifies the inherent noise in the realized quantum channel. The transformation acts as controllable leverage in the protocol—while it limits the information of an eavesdropper, it also amplifies the

effects of noise and eavesdropping. Thus, it may not be practical to reduce the maximal information of an eavesdropper to its minimum, since the noise may be amplified too much. However, the amplification of the noise does not reduce the benefits of the protocol substantially. Furthermore, as technology advances, the inherent noise of a quantum channel can be decreased. Studying the amplification of a channel noise in detail is a possible topic for future research.

In our protocol, an eavesdropper is assured to have only one-by-one access to the transmitted particles. We studied how much this, in general, restricts the capability of the eavesdropper of obtaining the transmitted entangled state. We maximized numerically the minimal error in approximating an entangled two-qubit state with a product state. We found that the maximum of the minimal error in the approximation is 0.673. Thus, even if the eavesdropper was equipped with a perfect quantum cloner, the proposed protocol would impose a significant hindrance to him or her.

In addition, we described a novel attack type against the proposed protocol and showed that it enables an eavesdropper to imitate the entanglement in the transmission. In this so-called EPR-pair attack, the eavesdropper captures the transmitted states and replaces them with the halves of an EPR pair. We showed that in a special case and under strong assumptions on the capabilities of the attacker and the entangling transformation, this attack allows the eavesdropper to gain full knowledge on the generated key. Note that these assumptions would render BB84 useless. Detailed investigation of this attack type is left for future research.

Suggestions for topics of future research also include the following. The security of the protocol could be analyzed in the presence of an attacker with more capabilities than what we have allowed. Firstly, the attacker can be allowed to measure the transmissions individually in any basis, implementable by allowing the use of arbitrary single-qubit gates, and to adjust each measurement based on previous results. Secondly, the security could be analyzed under an optimal incoherent attack, and, if possible, in the case of a collective attack. If the advantage is not lost under the most general attack, entangling the states of more than two particles would probably create an even larger advantage, since the dimension of an  $N$ -qubit state increases exponentially in  $N$ .

# Bibliography

- [1] D. Kahn, *The Codebreakers: The Story of Secret Writing* (New York: Scribner, 1996).
- [2] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 3rd Ed. (Upper Saddle River: Prentice Hall, 2003).
- [3] The Committee on National Security Systems,  
[http://www.cnss.gov/Assets/pdf/cnssp\\_15\\_fs.pdf](http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf), September 11th 2006.
- [4] S. Wiesner, SIGACT News **15**, 78 (1983).
- [5] A. Galindo and M. A. Martín-Delgado, Rev. Mod. Phys. **74**, 347 (2002).
- [6] G. Brassard, arXiv:quant-ph/0604072 (2006).
- [7] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE, 1984).
- [8] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
- [9] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
- [10] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
- [11] M. Genovese and C. Novero, Eur. Phys. J. D **21**, 109 (2002).
- [12] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
- [13] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [14] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
- [15] C. Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, Phys. Rev. Lett. **94**, 150501 (2005).
- [16] A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996).

- [17] D. Bouwmeester, A. Ekert, A. Zeilinger (Eds.), *The Physics of Quantum Information* (Berlin: Springer-Verlag, 2000).
- [18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [19] D. Welsh, *Codes and Cryptography* (Oxford: Oxford University Press, 1988).
- [20] G. Brassard and L. Salvail, Eurocrypt '93, Lofthus, Norway (1994).
- [21] Wikipedia, <http://en.wikipedia.org/wiki/Bit>, September 22nd 2006.
- [22] D. P. DiVincenzo, *Fortschr. Phys.* **48**, 771 (2000).
- [23] C. Elliott, D. Pearson, G. Troxel, SIGCOMM '03, August 25-29, Karlsruhe, Germany (2003).
- [24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press, 2001).
- [25] M. Christandl, arXiv:quant-ph/0604183 (2006).
- [26] W. K. Wootters, *Phys. Rev. Lett.* **80**, 2245 (1998).
- [27] V. Scarani, S. Iblisdir, and N. Gisin, *Rev. Mod. Phys.* **77**, 1225 (2005).
- [28] V. Bužek and M. Hillery, *Phys. Rev. A* **54**, 1844 (1996).
- [29] R. F. Werner, *Phys. Rev. A* **58**, 1827 (1998).
- [30] C.-S. Niu and R. B. Griffiths, *Phys. Rev. A* **58**, 4377 (1998).
- [31] N. J. Cerf, *Phys. Rev. Lett.* **84**, 4497 (2000).
- [32] N. J. Cerf, *J. Mod. Opt.* **47**, 187 (2000).
- [33] S. L. Braunstein, V. Bužek, and M. Hillery, *Phys. Rev. A* **63**, 052313 (2001).
- [34] S. Iblisdir, A. Acin, and N. Gisin, arXiv:quant-ph/0505152 (2005).
- [35] J. Fiurášek, R. Filip, and N. J. Cerf, *Quant. Inf. Comp.* **5**, 583 (2005).
- [36] C.-S. Niu and R. B. Griffiths, *Phys. Rev. A* **60**, 2764 (1999).
- [37] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, *Phys. Rev. A* **74**, 032330 (2006).
- [38] A. Acín, N. Gisin, and L. Masanes, *Phys. Rev. Lett.* **97**, 120405 (2006).
- [39] L.-P. Lamoureux, H. Bechmann-Pasquinucci, N. J. Cerf, N. Gisin, and C. Macchiavello, *Phys. Rev. A* **73**, 032304 (2006).



- [40] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
- [41] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
- [42] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
- [43] J. M. Renes, Quant. Inf. Comp. **5**, 081 (2005).
- [44] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, arXiv:quant-ph/0411022 (2004).
- [45] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
- [46] Y. C. Liang, D. Kaszlikowski, B.-G. Englert, L. C. Kwek, and C. H. Oh, Phys. Rev. A **68**, 022324 (2003).
- [47] J.-W. Lee, E. K. Lee, Y. W. Chung, H.-W. Lee, and J. Kim, Phys. Rev. A **68**, 012324 (2003).
- [48] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **67**, 062309 (2003).
- [49] G. A. Durkin, C. Simon, and D. Bouwmeester, Phys. Rev. Lett. **88**, 187902 (2002).
- [50] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
- [51] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, Phys. Rev. A **64**, 024302 (2001).
- [52] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306 (2001).
- [53] S. N. Molotkov and S. S. Nazin, JETP **92**, 871 (2001).
- [54] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
- [55] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
- [56] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
- [57] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
- [58] T. C. Ralph, Phys. Rev. A **61**, 010302 (1999).
- [59] G. Brassard, T. Mor, and C. Sanders, arXiv:quant-ph/9906074 (1999).
- [60] S. N. Molotkov, arXiv:quant-ph/9811038 (1998).
- [61] W. Y. Hwang, I. G. Koh, and Y. D. Han, Phys. Lett. A **244**, 489 (1998).

- [62] G. Ribordy, J.-D. Gautier, N. Gisin, O Guinnard, and H. Zbinden, *Electron. Lett.* **34**, 2116 (1998).
- [63] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, *Phys. Rev. A* **68**, 042331 (2003).
- [64] T.-Y. Chen, J. Zhang, J.-C. Boileau, X.-M. Jin, B. Yang, Q. Zhang, T. Yang, R. Laflamme, and J.-W. Pan, *Phys. Rev. Lett.* **96**, 150504 (2006).
- [65] L. P. Lamoureaux, E. Brainis, D. Amans, J. Barrett, and S. Massar, *Phys. Rev. Lett.* **94**, 050503 (2005).
- [66] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, *J. Mod. Opt.* **48**, 2009 (2001).
- [67] B. Darquié, M. P. A. Jones, J. Dingjan, J. Beugnon, S Bergamini, Y. Sortais, G. Messin, A. Browaeys, and P. Grangier, *Science* **309**, 454 (2005).
- [68] H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
- [69] P. M. Leung and T. C. Ralph, *Phys. Rev. A* **74**, 022311 (2006).
- [70] J. Sherson, A. S. Sørensen, J. Fiurášek, K. Mølmer, and E. S. Polzik, *Phys. Rev. A* **74**, 011802 (2006).
- [71] C. A. Fuchs and A. Peres, *Phys. Rev. A* **53**, 2038 (1996).
- [72] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, *Phys. Rev. A* **56**, 1163 (1997).
- [73] M. Koashi, *arXiv:quant-ph/0505108* (2005).
- [74] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Quantum Inf. Comput.* **4**, 325 (2004).
- [75] H. F. Chau, *Phys. Rev. A* **66**, 060302 (2002).
- [76] H. Inamori, N. Lütkenhaus, and D. Mayers, *arXiv:quant-ph/0107017* (2001).
- [77] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
- [78] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996) and *Phys. Rev. Lett.* **80**, 2022 (1998).
- [79] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [80] J. S. Bell, *Rev. Mod. Phys.* **38**, 447 (1966).
- [81] Mathematica version 5.1.0.0 by Wolfram Research, Inc., Advanced Documentation.
- [82] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, *Phys. Rev. A* **67**, 042313 (2003).